

University of Warwick institutional repository: <http://go.warwick.ac.uk/wrap>

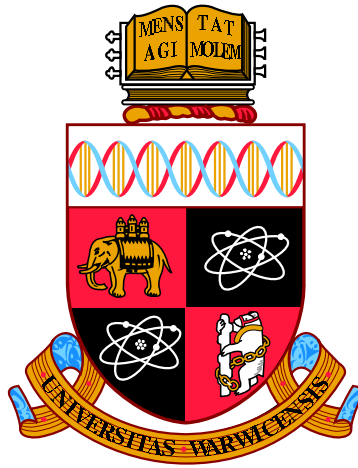
A Thesis Submitted for the Degree of PhD at the University of Warwick

<http://go.warwick.ac.uk/wrap/58400>

This thesis is made available online and is protected by original copyright.

Please scroll down to view the document itself.

Please refer to the repository record for this item for information to help you to cite it. Our policy information is available from the repository home page.



On Some Local to Global Phenomena for Abelian Varieties

by

Barinder Singh Banwait

Thesis

Submitted to The University of Warwick

for the degree of

Doctor of Philosophy

Mathematics Institute

September, 2013

THE UNIVERSITY OF
WARWICK

ਲਛਮਨ, ਪ੍ਰੇਮ ਲਤਾ, ਅਤੇ ਭੈਨਜੀ ਵਾਸਤੇ

For Lachhman, Prem Lata, and Bhenji

Table of Contents

Acknowledgments	iv
Declaration	v
Abstract	vi
1 Introduction	1
1.1 What is the <i>local to global principle</i> ?	1
1.2 The content of this thesis	4
1.3 Notation and conventions	5
2 The Local to Global Problem for Isogenies - Background	6
2.1 Preliminaries on abelian varieties and isogenies	6
2.2 Formulation of the Problem	10
2.3 Restriction to elliptic curves - a summary of Sutherland's work	14
2.4 Modular Curves	17
3 The Local to Global Problem for Isogenies - Development	21
3.1 Hasse curves in the trivial determinant case	21
3.2 A parametrisation of Hasse at 5 curves	24
3.3 Hasse curves over quadratic fields I: Sutherland-type pairs	28
3.4 Hasse curves over quadratic fields II: non Sutherland type pairs . . .	32
3.5 Fields admitting no exceptional pairs	34
3.6 From almost all to all	35
3.7 Hasse surfaces	38
4 The Hunt for Tetrahedral at 13 Elliptic Curves	42
4.1 $X_{S_4}(l)$ and $X_{A_4}(l)$	43
4.2 The equation for $X_{S_4}(13)$	45
4.3 Obtaining octahedral elliptic curves over \mathbb{Q}	46
4.3.1 Step 1. Compute the j -map	46
4.3.2 Step 2. Points on $X_{S_4}(13)$	50
4.3.3 Step 3. Evaluate j at these points	51
4.4 Modular curves of level 13 and genus 3	52

5	Computing $S_2(\Gamma_{A_4}(13))$ in 7 Steps	58
5.1	Step 1. Identifying our desired space as the invariants of a representation	58
5.2	Step 2. The conjugate representation	59
5.3	Step 3. Identifying the 3 relevant sub-representations	60
5.4	Step 4. Computing the action of $\mathrm{PSL}_2(\mathbb{F}_{13})$ upon each sub-representation	62
5.5	Step 5. Computing the action of \tilde{S} and \tilde{T}	62
5.6	Step 6. Computing the Atkin-Lehner pseudoeigenvalues	64
5.7	Step 7. The cuspforms	66
6	The Local to Global Problem for Torsion - Problem (2)	70
6.1	Formulation of the problem	70
6.2	Reformulation of the problem - the work of Katz	71
6.3	The case of modular abelian varieties	72
7	Conclusion	76
	Bibliography	78

Acknowledgments

This thesis would not have been possible without the constant support and encouragement of my adviser John Cremona. His energy and enthusiasm for number theory have been a source of great inspiration and an example to aspire to. I look back with joy at the many meetings and discussions we had, be it in his office, over coffee in the Maths Common Room, or during a skipped talk at a conference.

It is a true pleasure to thank Alex Bartel for always patiently and clearly addressing any of my queries, for his interest in my work and future plans, and above all for his warmth and friendship.

Special thanks are due to Jeroen Sijsling, whose help with the computations described in Chapter 4 was crucial and indispensable, and to Andrew Sutherland, for promptly addressing any concerns, as well as running several computations for me.

I am also very grateful to Samuele Anni, John Cullinan, Tim and Vladimir Dokchitser, Tom Fisher, David Loeffler, Martin Orr, Samir Siksek, Damiano Testa, and Liya and Lloyd Yu-West, for many helpful discussions and insightful suggestions.

I thank the Warwick Mathematics Institute for providing an excellent working environment, and the EPSRC for their financial support during my studies.

I deeply appreciate the constant love and support of my parents, which was so important during the writing of this thesis.

Finally I would like to thank Seema Oghra for being my first teacher of mathematics, and for inspiring me to continue pursuing it.

Declaration

Chapters 1 and 2 are expository. The results in the other chapters are my own work, unless otherwise indicated.

Abstract

Let A be an abelian variety over a number field K , which admits a K -rational l -isogeny, for l a prime. It is easy to show that, modulo every good prime $\mathfrak{p} \nmid l$, the reduced abelian variety $\tilde{A}_{\mathfrak{p}}$ has an $\mathbb{F}_{\mathfrak{p}}$ -rational l -isogeny. In this thesis we ask whether the converse of this statement holds: if $\tilde{A}_{\mathfrak{p}}$ has an $\mathbb{F}_{\mathfrak{p}}$ -rational l -isogeny for all good primes $\mathfrak{p} \nmid l$, then must A admit a K -rational l -isogeny? We focus mainly on the case of elliptic curves, extend recent work of Andrew Sutherland, give explicit examples for which the answer to the above question is “No”, and attempt to classify all such examples over quadratic fields. This leads us to find elliptic curves over $\mathbb{Q}(\sqrt{13})$ whose projective mod-13 Galois image is isomorphic to the alternating group A_4 , and to find an explicit model for the genus 3 modular curve $X_{S_4}(13)$ as a plane quartic in $\mathbb{P}_{\mathbb{Q}}^2$.

We also consider a related problem where “ l -isogeny” is replaced with “ l -torsion”: if $\tilde{A}_{\mathfrak{p}}$ has an $\mathbb{F}_{\mathfrak{p}}$ -rational l -torsion point for all good primes $\mathfrak{p} \nmid l$, then must A be K -isogenous to an abelian variety A' which admits a K -rational l -torsion point? We show that, if A is a modular abelian variety over \mathbb{Q} , then the answer is “Yes”.

Chapter 1

Introduction

1.1 What is the *local to global principle*?

One often hears the phrase *local to global principle* in mathematics, though especially in number theory and arithmetic geometry. Fundamental building blocks in these areas are spaces which admit infinitely many points of an “arithmetic nature”; the basic example is that of the integers \mathbb{Z} , where the infinitely many “arithmetic” points are the prime numbers. One then has an object, f say, defined over one of these spaces; think of a polynomial over the integers, for example. We’ll call this the **global object**. We also require there to exist a notion of “specialising” the object over each of the arithmetic points to get a “specialised”, or **local** object; think now about reducing that polynomial mod p . One also thinks of a property, P say, that the global object might satisfy; in our polynomial example, think of the property of being reducible. This property must be such that it makes sense for the corresponding local objects also to possess the property. For that polynomial, the property of being reducible is such a property; the property of having all coefficients positive, for instance, is not.

It is often the case that, if the global object f satisfies the property P , then so too do all of its specialisations. We say that the object f satisfies the **global to**

everywhere local principle for P , or even simply that it satisfies the **global to local principle for P** . Other times one cannot expect this for *all* specialisations, but merely for *most* specialisations; some small (though possibly infinite) number of specialisations are allowed to not satisfy the property. In such a case we might describe the situation by saying that f satisfies the **global to almost everywhere local principle for P** ; that's quite a mouthful, so, provided we bear this "almost everywhere" in mind when talking about this, we may again use the succinct form **global to local principle**.

As an example, it is clear, for a reducible *monic* polynomial, that *all* of its specialisations are also reducible - we may say that monic polynomials over the integers satisfy the global to everywhere local principle for reducibility. If however the polynomial is not monic, then the specialisations at the primes dividing the leading coefficient may not be reducible; consider $3x^2 + 5x + 2$, for example. This polynomial has *almost all* of its specialisations being reducible.

Whenever we have such a global to local situation, we may then ask the following question.

Question 1.1.1 (Local to global problem for P). *If all specialisations of f satisfy the property P , then must f also satisfy P ? (As above, by "all", we may mean "almost all".)*

If the answer is "Yes", we say that f **satisfies the local to global principle for P** ; otherwise we say that it **fails the local to global principle for P** . If every object in a class \mathcal{C} of objects satisfies the local to global principle for P , we say that \mathcal{C} **satisfies the local to global principle for P** .

Let us consider our running example; we have the class \mathcal{C} of monic polynomials over the integers, and P the property of being reducible. We may ask: Does \mathcal{C} satisfy the local to global principle for P ?

The answer is "No". Indeed, the polynomial

$$X^4 + 3X^2 + 7X + 4$$

is reducible mod p for every single prime p , but is irreducible over \mathbb{Z} . However, not every monic polynomial fails the local to global principle for P ; one may show, for example, that any degree 5 polynomial must satisfy the local to global principle for P .

These examples indicate a deeper challenge: given an object, how can one determine whether or not it satisfies the principle P ? What do all the failures of the principle have in common? Given a class of objects, we would like to understand **the obstruction** to them satisfying the local to global principle for P . We refer to this task as the **local to global problem for P** .

In our running example of integer polynomials and reducibility, the obstruction is explained via the Galois group. The polynomials f that fail the local to global principle must satisfy the following two conditions, and conversely, any polynomial satisfying these two conditions will be a failure.

- $\text{Gal}(f)$ acts transitively on the roots of f in an algebraic closure;
- $\text{Gal}(f)$ does not contain a cycle of order $\deg f$ when viewed as a permutation group on the roots of f .

This explains *why* the polynomial $X^4 + 3X^2 + 7X + 4$ fails the principle: its Galois group is A_4 , which satisfies the above two conditions. Our understanding of the obstruction also allows us to state attractive corollaries such as the following.

Corollary 1.1.2. *The local to global principle for reducibility holds for monic integer polynomials of prime degree.*

Corollary 1.1.3. *For every non-prime integer $n > 1$, there exist monic integer polynomials of degree n which fail the local to global principle for reducibility.*

1.2 The content of this thesis

In this thesis we will be studying two related local to global problems. Our objects in all cases will be **abelian varieties over number fields**, and the two properties will be as follows; l denotes a fixed prime number.

1. Possesses an l -isogeny rational over the basefield.
2. Possesses an l -torsion point rational over the basefield.

We will take care to formulate the problems properly, especially in case (2), to pre-empt the trivial counterexamples. We must also give an overview of the extensive work that has already been done on both of these problems, for they will serve as our point of departure.

This thesis will unfortunately not give a full answer, or impart full understanding, to either of these problems. It will however extend what is currently known about them, in various different directions. Along the way will arise some other phenomena that are of interest in their own right.

Here is a more detailed overview of what the thesis entails. Chapter 2 is an expository chapter giving the basics on abelian varieties and modular curves, stating the local to global problem for (1) above, and summarising the work of Andrew Sutherland on this problem in the special case of elliptic curves.

Chapter 3 begins our own development in the elliptic curve case; we give a group theoretic criterion for elliptic curves to satisfy the local to global principle for (1) in the cases which Sutherland did not consider (Proposition 3.1.4). We give an infinite family of failures of the local to global principle for $l = 5$ in Theorem 3.2.2, and we parametrise their j -invariants. We then attempt to classify all failures of the principle over quadratic fields; this classification is still incomplete, though we reduce it to Conjecture 3.3.5, Question 3.4.3, and Question 3.4.4. Thereafter we consider the phenomenon of number fields admitting *no* failures of the principle; see

Proposition 3.5.2. The section ends with remarks and a survey of what is known in the dimension 2 case of the problem; we in particular consider the class of **modular abelian varieties**, and show (Proposition 3.7.7) that, for these varieties, the study of the local to global problem for (1) above reduces essentially to the case of elliptic curves.

Chapters 4 and 5 are devoted to answering Question 3.4.3. This leads to the main result of this thesis (see Theorem 4.0.9).

Theorem. *There exist elliptic curves over $\mathbb{Q}(\sqrt{13})$ whose projective mod-13 Galois image is isomorphic to A_4 ; these are also failures of the local to global principle for 13-isogenies for elliptic curves over $\mathbb{Q}(\sqrt{13})$.*

Chapter 6 starts on the local to global problem for (2) above. After presenting the problem and the work of Nick Katz on it, we state our goal in Section 6.3, and prove that the local to global principle for (2) holds for modular abelian varieties (Theorem 6.3.1).

1.3 Notation and conventions

We mostly use standard notation throughout. We will sometimes refer to elliptic curves by their *Cremona label*; thus, when we say “the elliptic curve 389a1”, for example, we mean the rational elliptic curve with label 389a1 in Cremona’s database of elliptic curves (see the *L-functions and Modular Forms Database* at <http://www.lmfdb.org> for an interactive version of the tables).

We often refer to computations carried out with the software packages **Sage** (see [S⁺13]) and **Magma** (see [BCP97]).

The label “Question” is used extensively throughout this thesis. Some of these are questions we answer fully or in part, but most are questions not dealt with at all in this thesis. We have either explicitly written which is the case, or we hope that the context makes clear which is the case.

Chapter 2

The Local to Global Problem for Isogenies - Background

2.1 Preliminaries on abelian varieties and isogenies

We assume the reader is familiar with the basic properties of varieties over a field; this is explained for example in Chapter 1, §1-3 of [Har77], or Chapter 4 of [Mil09]. In particular, the varieties over a given field form a category, in which products exist. Throughout this section K will denote an arbitrary perfect field, l will denote any prime, and N will denote any positive integer.

Let V be a variety over K . By a **point** of V we mean a geometric point, a point defined over \overline{K} . By a **K -point** of V we mean a point defined over K .

Let V, W be two varieties over K . Let $\phi : V \rightarrow W$ be a morphism of varieties defined over \overline{K} . ϕ induces a map on the function fields

$$\phi^* : \overline{K}(W) \rightarrow \overline{K}(V)$$

which, being a homomorphism of fields, is necessarily injective; for ease of notation we identify $\overline{K}(W)$ with its image under ϕ^* . We say that ϕ is **finite** if the extension of

fields $\overline{K}(V)/\overline{K}(W)$ is a finite extension, and in this case we may define the **degree** of ϕ to be the degree of this field extension:

$$\deg(\phi) := [\overline{K}(V) : \overline{K}(W)].$$

We say that ϕ is **separable** if this extension of fields is separable. Separability of ϕ is automatic if $\text{char } K = 0$; for positive characteristic, one may show that, if $\text{char } K \nmid \deg(\phi)$, then ϕ is separable.

We say that a variety is **connected** if it is connected as a topological space (with the Zariski topology). We say a variety V is **complete** if for all varieties W , the natural projection $V \times W \rightarrow W$ is a closed map, that is, it sends closed subsets to closed subsets.

Within the category of varieties over a field we may consider the group objects; these are called **group varieties**. This means that, if V is a group variety, then it comes equipped with a triple (m_V, ι_V, e_V) where

$$m_V : V \times V \rightarrow V$$

is a morphism of varieties called multiplication,

$$\iota_V : V \rightarrow V$$

is a morphism of varieties called inverse, and $e_V \in V(K)$ is an element such that the structure on $V(\overline{K})$ defined by m_V and ι_V is a group with identity e_V .

By an **abelian variety** we mean a group variety which is complete and connected. We may consider the category of abelian varieties over a field (as a subcategory of the category of varieties over the field); the morphisms in this subcategory are then the morphisms of varieties $A \xrightarrow{\alpha} B$ which respect the multiplication and inverse morphisms of A and B ; that is, we require the following diagrams to com-

mute:

$$\begin{array}{ccc}
 A \times A & \xrightarrow{(\alpha, \alpha)} & B \times B \\
 m_A \downarrow & & \downarrow m_B \\
 A & \xrightarrow{\alpha} & B
 \end{array}
 \quad \text{and} \quad
 \begin{array}{ccc}
 A & \xrightarrow{\alpha} & B \\
 \iota_A \downarrow & & \downarrow \iota_B \\
 A & \xrightarrow{\alpha} & B
 \end{array}$$

Henceforth in this section, A will denote any abelian variety over K . As the name suggests, the set $A(\overline{K})$ of points of A form an *abelian* group, though this is a non-trivial result requiring a proof (which can be found as Corollary 1.4 in [Mil08]; it is a consequence of the *Rigidity Theorem*).

Let P, Q be two points on A . Instead of writing $m_A(P, Q)$, we simply write $P + Q$. Instead of writing e_A , we simply write 0 . Instead of writing $P + \dots + P$ with N summands, we simply write $N \cdot P$. We may consider the **points of order N** of A :

$$A[N] := \{P \in A(\overline{K}) : N \cdot P = 0\},$$

and note that it is the kernel of the morphism

$$[N] : A \longrightarrow A$$

$$P \longmapsto N \cdot P.$$

By an **isogeny on A** we mean a morphism of abelian varieties $\phi : A \rightarrow B$ which is surjective and has finite kernel; B is any other abelian variety defined over \overline{K} (and not necessarily defined over K). It is proved in Proposition 7.1 of [Mil08] that an isogeny is finite, and so by the above discussion we may associate to any isogeny a degree. If K is algebraically closed, and the isogeny ϕ is separable, then one may show that every fibre of ϕ has exactly $\deg(\phi)$ points - in particular, the kernel has exactly $\deg(\phi)$ points. By an N -isogeny we mean an isogeny of degree N . We will usually be working in the case where $\text{char } K = 0$, or $\text{char } K \nmid N$, so by the remark above, our N -isogenies will usually be separable. Thus, unless otherwise specified,

we henceforth assume all isogenies are separable.

We may consider the set of (separable!) l -isogenies on A , and denote it by Ω_l . This set admits a natural action of $G_K := \text{Gal}(\overline{K}/K)$, which we now describe. Let $\phi \in \Omega_l$, and $\sigma \in G_K$. Then ϕ is a morphism from A to B say, where B is defined over \overline{K} . We define ϕ^σ to be the map making the following diagram commute:

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ \sigma \downarrow & & \downarrow \sigma \\ A & \xrightarrow{\phi^\sigma} & B^\sigma; \end{array}$$

i.e., $\phi^\sigma = \sigma \phi \sigma^{-1}$. B^σ is the conjugated abelian variety, and note that this is indeed an isogeny on A in the above sense.

We may also consider the set of order l subgroups of $A(\overline{K})$; any such subgroup must be contained in $A[l]$, and indeed the set of these subgroups is equal to $\mathbb{P}(A[l])$, the **projectivisation**¹ of $A[l]$. Since $A[l]$ admits a natural G_K -action (given by the Galois action on the points), we obtain a G_K -action on $\mathbb{P}(A[l])$.

Lemma 2.1.1. *There is a bijection of G_K -sets*

$$\begin{aligned} \Omega_l &\longrightarrow \mathbb{P}(A[l]) \\ \phi &\longmapsto \ker \phi \\ (A \rightarrow A/C) &\longleftarrow C. \end{aligned}$$

By A/C , we mean the quotient of A by C , where C is regarded as a finite group of automorphisms of A .

Remark 2.1.2. See Theorem 1 in §7 of [Mum74] for more details on the construction of quotients of varieties by finite groups of automorphisms.

¹The projectivisation of an abelian group G is the underlying set of G , modulo the equivalence relation that two elements are identified if one is a multiple of the other under the group law.

Proof. That the kernel of an l -isogeny has size l was remarked above. Conversely, given an order l subgroup C of $A[l]$, one may construct a unique l -isogeny from A to another abelian variety A' , whose kernel is C ; this converse is proved in Theorem 4, §7 of [Mum74]. \square

We say that an l -isogeny is **K -rational** if it is fixed by the G_K action.

2.2 Formulation of the Problem

In this section we will consider an abelian variety A over a *number field* K . We still have the bijection of (2.1.1), but we now make the G_K action on $\mathbb{P}(A[l])$ very concrete by choosing a basis for $A[l]$ as an \mathbb{F}_l -vector space. We have a group isomorphism

$$A[l] \cong (\mathbb{Z}/l\mathbb{Z})^{2d},$$

where d is the dimension of A . We fix such a group isomorphism. We then have the following commutative diagram.

$$\begin{array}{ccccc} G_K & \xrightarrow{\quad} & \mathrm{GL}(A[l]) & \xrightarrow{\sim} & \mathrm{GL}_{2d}(\mathbb{F}_l) \\ & \searrow & \downarrow & & \downarrow \\ & & \mathrm{GL}(\mathbb{P}(A[l])) & \xrightarrow{\sim} & \mathrm{PGL}_{2d}(\mathbb{F}_l). \end{array}$$

We let $\bar{\rho}_{A,l}$ be the homomorphism from G_K to $\mathrm{GL}_{2d}(\mathbb{F}_l)$, and $\mathbb{P}\bar{\rho}_{A,l}$ the map from G_K to $\mathrm{PGL}_{2d}(\mathbb{F}_l)$. If A and l are understood, we will denote $\mathbb{P}\bar{\rho}_{A,l}$ simply as ρ .

We let $G_{A,l}$ denote the image of $\bar{\rho}_{A,l}$, and $H_{A,l}$ denote the image of ρ ; by the commutativity of the above diagram, $H_{A,l}$ is equal to $G_{A,l}$ modulo the scalar matrices. $G_{A,l}$ acts faithfully on \mathbb{F}_l^{2d} , and $H_{A,l}$ acts faithfully on $\mathbb{P}(\mathbb{F}_l^{2d}) = \mathbb{P}^{2d-1}(\mathbb{F}_l)$. A different choice of isomorphism changes $G_{A,l}$ and $H_{A,l}$ by conjugation, so the conjugacy class of these subgroups is independent of the choice of isomorphism made. We refer to $G_{A,l}$ as the **mod- l Galois image** of A , and $H_{A,l}$ as the **projective mod- l**

Galois image.

The G_K action on $\mathbb{P}(A[l])$ is now described concretely as the $H_{A,l}$ action on $\mathbb{P}^{2d-1}(\mathbb{F}_l)$, which is just the action of matrix multiplication (of a finite matrix group) on column vectors modulo scaling.

In particular, an l -isogeny is **K -rational** if and only if the associated point of $\mathbb{P}^{2d-1}(\mathbb{F}_l)$ is fixed by $H_{A,l}$ (This latter property depends only on the conjugacy class of $H_{A,l}$, and so is independent of the choice of isomorphism made).

Remark 2.2.1. If A admits a polarisation of degree coprime to l , then the image of $G_K \rightarrow \mathrm{GL}(A[l])$ is actually contained in $\mathrm{GSp}(A[l])$; this is a consequence of the existence of the **Weil pairing** on $A[l]$, and the fact that it is Galois equivariant, non-degenerate, and symplectic. Thus, in this case, we may regard $G_{A,l}$ and $H_{A,l}$ as subgroups of $\mathrm{GSp}_{2d}(\mathbb{F}_l)$ and $\mathrm{PGSp}_{2d}(\mathbb{F}_l)$ respectively. In this thesis, we will always assume this symplectic structure.

Attached to A is a finite set of primes of K , called the *bad primes for A* , whose definition we now recall (see Chapter 2, §2 of [Mil08], or [ST68] for more details). Let \mathfrak{p} be a prime of K , and consider the local field $K_{\mathfrak{p}}$. Let $A_{K_{\mathfrak{p}}}$ denote the basechange of A to $K_{\mathfrak{p}}$, and embed $A_{K_{\mathfrak{p}}}$ into a projective space \mathbb{P}^n ; corresponding to $A_{K_{\mathfrak{p}}}$ is an ideal I of $K_{\mathfrak{p}}[X_1, \dots, X_n]$. Let $\mathbb{Z}_{\mathfrak{p}}$ denote the valuation ring of $K_{\mathfrak{p}}$, and $\mathbb{F}_{\mathfrak{p}} := \mathbb{Z}_{\mathfrak{p}}/\mathfrak{p}\mathbb{Z}_{\mathfrak{p}}$ the residue field. Let I_0 be the image of $I \cap \mathbb{Z}_{\mathfrak{p}}[X_1, \dots, X_n]$ inside $\mathbb{F}_{\mathfrak{p}}[X_1, \dots, X_n]$. This defines a variety A_0 over $\mathbb{F}_{\mathfrak{p}}$, which may be singular, and may depend on the choice of projective embedding. If, however, it is nonsingular, then it is independent of the choice, and is again an abelian variety. In this case we say that A has *good reduction at \mathfrak{p}* , and we write $\tilde{A}_{\mathfrak{p}}$ instead of A_0 for the reduced abelian variety. If A does not have good reduction at \mathfrak{p} , then we say that A has *bad reduction at \mathfrak{p}* , and we say that \mathfrak{p} is a *bad prime for A* . This set of bad primes is a finite set.

Let S be the following finite set of primes of K :

$$S := \{\text{bad primes for } A\} \cup \{\mathfrak{p} | l\}.$$

We define $G_{K,S} := \text{Gal}(\overline{K}_S/K)$, where \overline{K}_S is the maximal algebraic extension of K in \overline{K} which is unramified outside of S . This is a quotient of G_K , and it is a standard application of the criterion of Néron-Ogg-Šafarevič (Theorem 1 in [ST68]) that the action of G_K on $A[l]$, and hence on $\mathbb{P}(A[l])$ and Ω_l , factors through $G_{K,S}$.

For each prime \mathfrak{p} of K not in S , we fix an embedding of \overline{K} inside $\overline{K}_{\mathfrak{p}}$; such a choice allows us to identify $G_{\mathbb{F}_{\mathfrak{p}}}$ with a subgroup $D(\mathfrak{p})$ of $G_{K,S}$; in particular, there is an element $\text{Frob}_{\mathfrak{p}}$ of $G_{K,S}$ which corresponds to the $|\mathbb{F}_{\mathfrak{p}}|$ -power Frobenius element of $G_{\mathbb{F}_{\mathfrak{p}}}$.

In particular, it makes sense to speak of an l -isogeny on A being fixed by $\text{Frob}_{\mathfrak{p}}$.

We may also reduce A modulo \mathfrak{p} to obtain the reduced abelian variety $\tilde{A}_{\mathfrak{p}}$ defined over $\mathbb{F}_{\mathfrak{p}}$.

The groups $A[l]$ and $\tilde{A}_{\mathfrak{p}}[l]$ are both isomorphic to $(\mathbb{Z}/l\mathbb{Z})^{2d}$. The former admits an action of $G_{K,S}$, the latter admits an action of $G_{\mathbb{F}_{\mathfrak{p}}}$. Restricting the action of $G_{K,S}$ on the former to $D(\mathfrak{p})$, and identifying as above the groups $G_{\mathbb{F}_{\mathfrak{p}}}$ and $D(\mathfrak{p})$, we have that the $G_{\mathbb{F}_{\mathfrak{p}}}$ -modules $A[l]$ and $\tilde{A}_{\mathfrak{p}}[l]$ are isomorphic. In particular, the reduction $\tilde{A}_{\mathfrak{p}}$ admits an $\mathbb{F}_{\mathfrak{p}}$ -rational l -isogeny if and only if A has an l -isogeny fixed by $\text{Frob}_{\mathfrak{p}}$.

Lemma 2.2.2. *A has an l -isogeny fixed by $\text{Frob}_{\mathfrak{p}}$ for all $\mathfrak{p} \notin S$ if and only if every element of $H_{A,l}$ admits a fixed point in $\mathbb{P}^{2d-1}(\mathbb{F}_l)$.*

Proof.

$$\begin{aligned} \forall \mathfrak{p} \notin S, A \text{ has } l\text{-isogeny fixed by } \text{Frob}_{\mathfrak{p}} &\iff \forall \mathfrak{p} \notin S, \Omega_l \text{ has a point fixed by } \text{Frob}_{\mathfrak{p}} \\ &\iff \forall \mathfrak{p} \notin S, \mathbb{P}(A[l]) \text{ has a point fixed by } \text{Frob}_{\mathfrak{p}} \\ &\iff \forall \mathfrak{p} \notin S, \mathbb{P}^{2d-1}(\mathbb{F}_l) \text{ has a point fixed by } \rho(\text{Frob}_{\mathfrak{p}}). \end{aligned}$$

We claim that this last assertion is equivalent to the statement that, for all $h \in H_{A,l}$, there is a point in $\mathbb{P}^{2d-1}(\mathbb{F}_l)$ fixed by h . The reverse implication is clear; the forward implication follows from the Chebotarëv density theorem, which allows

one to write each $h \in H$ as the image under ρ of at least one $\text{Frob}_{\mathfrak{p}}$ (indeed, a positive density of $\text{Frob}_{\mathfrak{p}}$). \square

Corollary 2.2.3. *If A admits a K -rational l -isogeny, then for all $\mathfrak{p} \notin S$, the reduction $\tilde{A}_{\mathfrak{p}}$ admits an $\mathbb{F}_{\mathfrak{p}}$ -rational l -isogeny.*

We think of this corollary as expressing a **global implies local** statement, as in the introduction. We are now ready to state one of the problems to be considered in this thesis.

Question 2.2.4. *Does the converse of the corollary hold? That is, given an abelian variety A of dimension d over a number field K such that, for all $\mathfrak{p} \notin S$, the reduction $\tilde{A}_{\mathfrak{p}}$ has an $\mathbb{F}_{\mathfrak{p}}$ -rational l -isogeny, does it follow that A has a K -rational l -isogeny? Equivalently, if every element of $H_{A,l}$ fixes a point of $\mathbb{P}^{2d-1}(\mathbb{F}_l)$, is there a point of $\mathbb{P}^{2d-1}(\mathbb{F}_l)$ fixed by all of $H_{A,l}$?*

In a slogan, we are asking if a certain **local to global** principle holds for the existence of rational l -isogenies on abelian varieties. The equivalent formulation reveals how the question depends only upon the projective mod- l Galois image of A .

As we will see in the next section, the answer to the question is “No”. We are therefore justified in introducing the following terminology.

- We say that an abelian variety A over a number field K is a **Hasse variety at l** if it does not satisfy this principle; i.e., that, for all $\mathfrak{p} \notin S$, the reduction $\tilde{A}_{\mathfrak{p}}$ admits an $\mathbb{F}_{\mathfrak{p}}$ -rational l -isogeny, but the variety A itself does not admit a K -rational l -isogeny.
- We say that A is a **Hasse variety** (without reference to a specific prime) if it is a Hasse variety at l for some prime l .
- If we fix a number field K , we say that a prime l is a **Hasse prime for K** if there exists an abelian variety over K which is Hasse at l .

- We say that a subgroup H of $\mathrm{PGSp}_{2d}(\mathbb{F}_l)$ is **Hasse** if its action on $\mathbb{P}^{2d-1}(\mathbb{F}_l)$ does not admit a fixed point, but every element of H does have a fixed point. A subgroup of $\mathrm{GSp}_{2d}(\mathbb{F}_l)$ is **Hasse** if its image in $\mathrm{PGSp}_{2d}(\mathbb{F}_l)$ is Hasse.

The last definition is introduced to make the following statement which highlights the group theoretic heart of the problem.

Corollary 2.2.5. *An abelian variety A over a number field K is Hasse at l if and only if the projective mod- l Galois image $H_{A,l}$ is Hasse.*

2.3 Restriction to elliptic curves - a summary of Sutherland's work

We now set the dimension of the abelian variety to be 1. One may easily check that, if $l = 2$, then no subgroup of $\mathrm{PGL}_2(\mathbb{F}_l)$ satisfies the Hasse condition. Thus, henceforth, **we will deal exclusively with odd primes**. We refer to a **Hasse curve at l** , or a **Hasse at l curve**, to be a Hasse variety at l of dimension 1. These were studied recently by Andrew Sutherland ([Sut12]), and we here give an overview of Sutherland's paper.

Observe that whether an elliptic curve over any perfect field k admits a k -rational isogeny or not depends only on its j -invariant. Thus, if E is a Hasse at l curve over a number field K , then so too is any elliptic curve E' with j -invariant $j(E)$. Hence one may define the notion of an **exceptional pair for a number field K** as a pair (l, x) for l a rational prime, and $x \in K$ such that there is a Hasse at l curve with j -invariant x . We may also refer to the x -coordinate of an exceptional pair as a **Hasse value** for K and l .

Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_l)$ whose reduction modulo scalar matrices is $H \subseteq \mathrm{PGL}_2(\mathbb{F}_l)$. We have the following commutative diagram:

$$\begin{array}{ccc}
G & \xrightarrow{\det} & \mathbb{F}_l^* \\
\downarrow & & \downarrow \\
H & \longrightarrow & (\mathbb{F}_l^*)/(\mathbb{F}_l^*)^2
\end{array}
;$$

by a slight abuse of notation, we refer to the bottom horizontal map also by \det . Observe that the image of \det on H is either trivial or surjective, because $(\mathbb{F}_l^*)/(\mathbb{F}_l^*)^2$ is a cyclic group of order 2.

If H is the whole of $\mathrm{PGL}_2(\mathbb{F}_l)$, then we define the kernel of \det on H to be $\mathrm{PSL}_2(\mathbb{F}_l)$; this is isomorphic to $\mathrm{SL}_2(\mathbb{F}_l)/\{\pm I\}$.

Thus, for a general subgroup $H \subseteq \mathrm{PGL}_2(\mathbb{F}_l)$, the dichotomy of whether or not it has trivial determinant may equivalently be expressed as whether or not it is contained in $\mathrm{PSL}_2(\mathbb{F}_l)$.

Sutherland classifies Hasse subgroups H of $\mathrm{PGL}_2(\mathbb{F}_l)$ under the assumption that $\det H$ is surjective.

Proposition 2.3.1 (Sutherland). *Let H be a Hasse subgroup of $\mathrm{PGL}_2(\mathbb{F}_l)$ with surjective determinant. Then*

1. H is dihedral of order $2n$, where $n > 1$ is an odd divisor of $(l-1)/2$;
2. The pullback G of H to $\mathrm{GL}_2(\mathbb{F}_l)$ is properly contained in the normaliser of a split Cartan subgroup;
3. $l \equiv 3 \pmod{4}$;
4. There is an element of $\mathbb{P}^1(\mathbb{F}_l)$ fixed by $\ker \det$, an index two subgroup of H .

Remark 2.3.2. Items (1) and (3) here imply items (2) and (4). Also, the converse to this proposition is also true; we will prove this in the next chapter.

If the subgroup H of $\mathrm{PGL}_2(\mathbb{F}_l)$ is the projective mod- l Galois image $H_{E,l}$ of an elliptic curve E over a number field K , then the condition that $\det H_{E,l}$ is surjective may be given an alternative description. To express this, we define $l^* := \pm l$, where

the $+$ sign is taken if l is congruent to 1 mod 4, and the $-$ sign otherwise. Note that the unique quadratic subfield of the cyclotomic field $\mathbb{Q}(\zeta_l)$ is precisely $\mathbb{Q}(\sqrt{l^*})$.

In the following Lemma, by $\mathrm{GL}_2^+(\mathbb{F}_l)$, we mean the subgroup of matrices with square determinant.

Lemma 2.3.3. *Let E/K be an elliptic curve. The following are equivalent.*

1. $H_{E,l} \subseteq \mathrm{PSL}_2(\mathbb{F}_l)$;
2. $\sqrt{l^*} \in K$;
3. $G_{E,l} \subseteq \mathrm{GL}_2^+(\mathbb{F}_l)$.

Proof. The equivalence of (1) and (3) is clear. The equivalence of (2) and (3) follows from standard Galois theory upon observing that the determinant of $\bar{\rho}_{E,l}$ is equal to the mod- l cyclotomic character over K . \square

In this way, Sutherland arrives at his first main theorem:

Theorem 2.3.4 (Theorem 1 in [Sut12]). *Let l be a prime, K a number field not containing $\sqrt{l^*}$, and E/K an elliptic curve over K . Suppose that, locally at a density one set of primes, the reduction $\tilde{E}_{\mathfrak{p}}$ has an $\mathbb{F}_{\mathfrak{p}}$ -rational l -isogeny. Then E has a $K(\sqrt{l^*})$ -rational l -isogeny. Moreover, if $l < 7$ or $l \equiv 1 \pmod{4}$, then the local to global principle for isogenies holds, that is, E has a K -rational l -isogeny.*

Sutherland's second theorem concerns explicitly finding the Hasse curves over \mathbb{Q} , that is, the exceptional pairs for \mathbb{Q} . Sutherland's first theorem implies that the exceptional primes must satisfy $l \geq 7$ and $l \equiv 3 \pmod{4}$. Sutherland shows that, if E has CM, then 7 is the only possible exceptional prime. If E does not have CM, then very recent work of Bilu, Parent and Rebolledo ([BPR11]) says that, for the mod- l image to satisfy the condition (2) in (2.3.1), then l must be 2,3,5,7 or 13. Therefore, the only possible exceptional prime for \mathbb{Q} is 7.

Now the question becomes: is there indeed a Hasse at 7 curve over \mathbb{Q} ? Sutherland's strategy towards this question is to construct the **moduli space of elliptic curves** which are Hasse at 7 (we will discuss moduli spaces of elliptic curves more in the next section); \mathbb{Q} -rational points of this moduli space correspond to ($\bar{\mathbb{Q}}$ -isomorphism classes of) Hasse at 7 curves. With the help of Noam Elkies, this moduli space is found to be the elliptic curve 49a3:

$$E : y^2 + y = x^3 - 20x + 43;$$

this curve has two rational points, which correspond to Hasse at 7 curves over \mathbb{Q} . The j -invariants of each of these corresponding curves is computed, and in both cases is $\frac{2268945}{128}$. Thus, $(7, \frac{2268945}{128})$ is the only exceptional pair for \mathbb{Q} , which is exactly Sutherland's Theorem 2.

In the next chapter we begin our own development of this theme by first investigating what happens in the case where $\det H_{E,l}$ is trivial. Before that, however, we would like briefly to discuss moduli spaces of elliptic curves.

2.4 Modular Curves

Let $N \geq 2$ be an integer, G a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, and K a number field. Consider the problem of finding some or all elliptic curves E over K whose $G_{E,N}$ is conjugate to G . We would like to construct an object which parametrises these elliptic curves.

Such an object does indeed exist, though one must be rather specific by what "parametrises" means. What *does* exist is an object $X_G(N)$, a smooth projective curve defined over a number field $M_{G,N}$, whose L -points, for L any extension of $M_{G,N}$, correspond to $\bar{\mathbb{Q}}$ -isomorphism classes of elliptic curves E defined over L whose mod- N G_L -representation is *contained in* (and not necessarily equal to) a conjugate

of G . What does not necessarily exist is an object classifying \mathbb{Q} -isomorphism classes of such objects. One way of understanding these existence/non-existence assertions is to use the **formalism of moduli problems** as discussed in Chapter 4 of [KM84]; in their language, one says that a **coarse moduli space** always exists, though a **fine moduli space** need not exist.

Here are some important facts about the curve $X_G(N)$:

- $M_{G,N} = \mathbb{Q}(\zeta_N)^{\det G}$, the subfield of the mod- N cyclotomic field fixed by $\det G$. In particular, $M_{G,N} = \mathbb{Q}$ if and only if $\det G$ is surjective.
- The genus of $X_G(N)$ can be worked out by an application of the Riemann-Hurwitz genus formula. An explicit formula in the case $N = l$ prime is given below.
- The j -invariant of an elliptic curve corresponding to a point on $X_G(N)$ can be obtained by evaluating the j -map at that point:

$$X_G(N) \xrightarrow{j} X(1) \cong \mathbb{P}^1.$$

j is a rational function on $X_G(N)$ and so can, at least in principle, be written down explicitly (relative to an explicit model for $X_G(N)$).

- As a curve over $\overline{\mathbb{Q}}$, $X_G(N)$ depends only on $G \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. In fact, over \mathbb{C} , $X_G(N)$ has the classical description as being a quotient of \mathcal{H}^* , the extended upper-half plane, by a congruence subgroup $\Gamma_G(N)$:

$$X_G(N)_{\mathbb{C}} \cong \Gamma_G(N) \backslash \mathcal{H}^*.$$

By $\Gamma_G(N)$, we mean the pullback to $\mathrm{SL}_2(\mathbb{Z})$ of $G \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ under the reduction mod N map.

The following is a master formula for computing the genus of $X_G(l)$, for l a prime, which can be found in [Lig76]; we write \overline{G} for $G \cap \mathrm{SL}_2(\mathbb{F}_l)$.

$$\mathrm{genus}(X_G(l)) = 1 + \frac{\mu_G}{12} - \frac{e_{2,G}}{4} - \frac{e_{3,G}}{3} - \frac{e_{\infty,G}}{2},$$

where

- $e_{\infty,G}$ is the number of cusps of $X_G(l)$;

-

$$e_{2,G} = \frac{l - \left(\frac{-1}{l}\right)}{\#\overline{G}} \# \{h \in \overline{G} : \mathrm{tr}(h) = 0\};$$

-

$$e_{3,G} = \frac{l - \left(\frac{-3}{l}\right)}{\#\overline{G}} \# \{h \in \overline{G} : \mathrm{tr}(h) = -1\}.$$

Example 2.4.1. Some groups G are more natural than others, and in these cases we do not write $X_G(N)$.

- If G is trivial, then we simply drop G from the notation, and write $X(N)$.
- If G is all of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, then we simply get $X(1)$, the moduli space parametrizing all elliptic curves up to twist.
- If G is the Borel subgroup of upper triangular matrices, then we write $X_0(N)$. This is the coarse moduli space of elliptic curves possessing a rational N -isogeny; moreover, instead of $\Gamma_G(N)$, we write $\Gamma_0(N)$.
- If G is the Borel subgroup of upper triangular matrices with a 1 in the top-left corner, then we write $X_1(N)$. This parametrises elliptic curves possessing a rational N -torsion point, and is in fact a fine moduli space; one writes $\Gamma_1(N)$ instead of $\Gamma_G(N)$.

The curve $X_0(N)$ admits an involution, called the Fricke involution. A point of $X_0(N)$ is represented by a pair (E, C) with E an elliptic curve, and C a Galois-

stable order- N subgroup of $E[N]$. The Fricke involution sends the pair (E, C) to $(E/C, E[N]/C)$; on the upper-half plane model, it maps z to $-\frac{1}{Nz}$.

Another important class of subgroups of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ are the **Cartan subgroups** and their normalisers, which we briefly mention here in the case $N = l$ prime; for a complete treatment see Chapter XVIII, §12 of [Lan02]. There are two sorts of Cartan subgroup, **split** and **non-split**. A split Cartan subgroup is conjugate to the group of diagonal matrices, and hence is isomorphic to $\mathbb{F}_l^* \times \mathbb{F}_l^*$. Its normaliser is then conjugate to the group C_s^+ of diagonal and antidiagonal matrices. A non-split Cartan subgroup is isomorphic to $\mathbb{F}_{l^2}^*$, and is conjugate to the group C_{ns} defined as follows:

$$C_{\mathrm{ns}} = \left\{ \begin{pmatrix} x & \delta y \\ y & x \end{pmatrix} : x, y \in \mathbb{F}_l, (x, y) \neq (0, 0) \right\},$$

where δ is any fixed quadratic non-residue in \mathbb{F}_l^* . It also has index two in its normaliser C_{ns}^+ . The matrices in C_s are diagonalisable over \mathbb{F}_l , whilst those in C_{ns} are not.

Associated to both of the groups C_s^+ and C_{ns}^+ are modular curves $X_s(l)$ and $X_{\mathrm{ns}}(l)$ respectively. The curve $X_s(l)$ is \mathbb{Q} -isomorphic to the quotient $X_0^+(l^2)$ of the modular curve $X_0(l^2)$ by the Fricke involution. Over \mathbb{C} , this isomorphism is established by mapping τ on $X_0^+(l^2)$ to $l\tau$ on $X_s(l)$.

Chapter 3

The Local to Global Problem for Isogenies - Development

3.1 Hasse curves in the trivial determinant case

Sutherland's group theoretic proposition (2.3.1) is not true in the trivial determinant case. We first identify where in Sutherland's argument the assumption of surjective determinant is used.

Sutherland begins his proof of (2.3.1) by proving the following.

Lemma 3.1.1 (Sutherland). *If $H \subseteq \mathrm{PGL}_2(\mathbb{F}_l)$ is Hasse, then $l \nmid \#H$.*

One may now use the following classical result.

Fact 3.1.2. *Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_l)$ of order prime to l , and let H be the image of G modulo scalars. Then one of the following holds.*

- (i) *H is cyclic and G is contained in a Cartan subgroup;*
- (ii) *H is dihedral and G is contained in the normaliser of a Cartan subgroup;*
- (iii) *H is **exceptional**; that is, isomorphic to A_4 , A_5 , or S_4 .*

Clearly no cyclic subgroup of $\mathrm{PGL}_2(\mathbb{F}_l)$ is Hasse, which rules out (i).

It is at this point that the assumption of surjective determinant is used: it allows Sutherland to rule out the exceptional case. Surjective determinant forces H to possess an index 2 subgroup (namely, the kernel of \det); since neither A_4 nor A_5 possess such a subgroup, they are eliminated. S_4 is excluded after rather more effort (see the proof of Lemma 1 in [Sut12]).

Thus, in the case of trivial determinant, we are forced to consider the possibility of H being exceptional. And these can certainly occur; recall that H having trivial determinant is equivalent to it being contained in $\mathrm{PSL}_2(\mathbb{F}_l)$.

Fact 3.1.3. *Let $l > 2$ be a prime.*

- $A_4 \subseteq \mathrm{PSL}_2(\mathbb{F}_l)$ for all l .
- $A_5 \subseteq \mathrm{PSL}_2(\mathbb{F}_l)$ if and only if $l \equiv \pm 1 \pmod{5}$.
- $S_4 \subseteq \mathrm{PSL}_2(\mathbb{F}_l)$ if and only if $l \equiv \pm 1 \pmod{8}$.

(A good reference for this well-known fact is the appendix, by Walter Feit, to Chapter XI of [Lan01].)

However, these exceptional subgroups will not always be Hasse. Determining when they are is given by the following result, which is the first contribution of this thesis.

Proposition 3.1.4. *A subgroup H of $\mathrm{PSL}_2(\mathbb{F}_l)$ is Hasse if and only if it satisfies one of the following four conditions:*

1. $l \equiv 1 \pmod{12}$, and $H \cong A_4$.
2. $l \equiv 1 \pmod{24}$, and $H \cong S_4$.
3. $l \equiv 1 \pmod{60}$, and $H \cong A_5$.
4. $l \equiv 1 \pmod{4}$, and $H \cong D_{2n}$ for $n > 1$ a divisor of $\frac{l-1}{2}$.

We begin with the following lemma.

Lemma 3.1.5. *Let $H \subseteq \mathrm{PSL}_2(\mathbb{F}_l)$ be Hasse, and let $h \in H$. Then the order of h must divide $\frac{l-1}{2}$.*

Proof. Let r denote the order of h which, by 3.1.1, must be coprime to l . Consider the cyclic group $H' := \langle h \rangle$, of order r . By 3.1.2, the pullback G' of H' to $\mathrm{GL}_2(\mathbb{F}_l)$ is contained in a Cartan subgroup. If this Cartan subgroup were non-split, then the elements of G' would *not* be diagonalisable, and hence h would fix no point of $\mathbb{P}^1(\mathbb{F}_l)$, contradicting the assumption that H is Hasse. Thus the Cartan subgroup must be split, so the elements of G' are diagonalisable; in particular, there is a basis in which h may be represented modulo scalar matrices by the matrix $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, for $a \in (\mathbb{F}_l^*)^2$. The lemma is proven by observing that the order of h is equal to the order of a . \square

The lemma proves the forward implication of 3.1.4; if $A_4 \subseteq \mathrm{PSL}_2(\mathbb{F}_l)$ is Hasse, then both 2 and 3 must divide $\frac{l-1}{2}$, and hence $l \equiv 1 \pmod{12}$. The other cases are similar.

We now show the converse. Let H be any of the groups listed in the above proposition (with the corresponding condition on l). Suppose, for a contradiction, that we have $h \in H$ which fixes no point of $\mathbb{P}^1(\mathbb{F}_l)$, let r be the order of this h , and let $s := |\mathbb{P}^1(\mathbb{F}_l)/h|$ be the number of orbits. Proposition 2 of [Sut12] says that $\mathrm{sign}(h) = (-1)^s$; in particular, s must be even. Applying the orbit counting lemma to the action of $\langle h \rangle$ on $\mathbb{P}^1(\mathbb{F}_l)$ yields the formula $s = (l+1)/r$, and hence r must divide $\frac{l+1}{2}$. However, an easy check reveals that every element of H , in all four cases, has order dividing $\frac{l-1}{2}$; in particular, r must divide both $\frac{l-1}{2}$ and $\frac{l+1}{2}$, which implies $r = 1$, and hence h must be the identity. But this contradicts the assumption that h fixes no point of $\mathbb{P}^1(\mathbb{F}_l)$.

The final step is to show that, for H as listed above, no point of $\mathbb{P}^1(\mathbb{F}_l)$ is fixed

by all of H . This follows from the following well-known fact from group theory; see for example Theorem 80.27 in [CR94].

Lemma 3.1.6. *Let G be a group, S a transitive left G -set, and H a subgroup of G . Denote by $H \backslash S$ the set of orbits of S under H . Let B denote the G -stabiliser of any point of S . Then we have an isomorphism of H -sets*

$$S \cong \bigsqcup_g H/(H \cap B^g),$$

where g runs over a set of double coset representatives for $H \backslash G/B$; here we regard the S on the left as an H -set.

We apply the lemma with $G = \mathrm{PSL}_2(\mathbb{F}_l)$, $S = \mathbb{P}^1(\mathbb{F}_l)$, and B the stabiliser of ∞ , that is, the Borel subgroup. By the lemma, an H -orbit of size 1 corresponds to a double coset representative g for which $H \subseteq B^g$. Since A_4 , S_4 and A_5 each contain a subgroup isomorphic to V_4 , and B does not, none of these three groups admit an orbit of size 1. If $H \cong D_{2n}$ for $n > 1$ a divisor of $\frac{l-1}{2}$, and a conjugate of H is contained in B , then the pullback of H to $\mathrm{GL}_2(\mathbb{F}_l)$ must simultaneously be contained in the normaliser of a split Cartan subgroup and a Borel subgroup; this would force H to be cyclic, which is a contradiction. Thus, in all four cases, there is no H -orbit of size 1.

Since an orbit of size 1 means a point of $\mathbb{P}^1(\mathbb{F}_l)$ fixed by all of H , we have finished the proof.

In the next sections, we will apply this group theoretic proposition to the problem of finding Hasse elliptic curves.

3.2 A parametrisation of Hasse at 5 curves

We now use the group theory of the previous section to answer the following question.

Question 3.2.1. *Does Sutherland's Theorem 1 hold without the assumption that $\sqrt{l^*} \notin K$?*

The answer is “No”. In particular, with Sutherland's assumption that $\sqrt{l^*} \notin K$, Sutherland's theorem says that 7 is the smallest Hasse prime. But we have the following result, which is joint work with John Cremona.

Theorem 3.2.2. *Let K be a number field containing $\sqrt{5}$. An elliptic curve E/K is Hasse at 5 if and only if its j -invariant is given by the formula*

$$j(s) = \frac{((s+5)(s^2-5)(s^2+5s+10))^3}{(s^2+5s+5)^5}$$

for some $s \in K$, together with the condition that all values of $t \in K$ for which $j(t) = j(s)$ satisfy $t^2 - 20$ is not a square in K .

Proof. By the proposition in the previous section, an elliptic curve E is Hasse at 5 over K if and only if $H_{E,5} \cong V_4$, the Klein 4 group. Thus, let E/K have $H_{E,5} \cong V_4$. It follows from Dickson's classification of subgroups of $\mathrm{GL}_2(\mathbb{F}_l)$ that $G_{E,5}$ is contained in the normaliser of a Cartan subgroup. If this Cartan subgroup were non-split, then $G_{E,5}$ would be contained in $C_{\mathrm{ns}}^+ \cap \mathrm{GL}_2^+(\mathbb{F}_5)$ (we may take the intersection by the assumption on K , see 2.3.3), and so $H_{E,5}$ would be contained in $(C_{\mathrm{ns}}^+ \cap \mathrm{GL}_2^+(\mathbb{F}_5))/\text{scalars}$, which is a group of size 6, and hence cannot contain a subgroup isomorphic to V_4 ; thus $G_{E,5} \subseteq C_s^+$, and so E/K corresponds to a K -point on the modular curve $X_s(5)$. The converse is not quite true; a K -point on $X_s(5)$ corresponds to an elliptic curve E' over K with $H_{E',5} \subseteq V_4$, and not necessarily equal to V_4 .

We now give an expression for the j -map $X_s(5) \xrightarrow{j} X(1)$. Since $X_0^+(25)$ is isomorphic to $X_s(5)$ under the map $\tau \mapsto 5\tau$, it suffices to write down the function $j(5\tau)$ in terms of a Hauptmodul s for $X_0^+(25)$.

Let t_N be a Hauptmodul for $X_0(N)$. Klein found the following formula in 1879.

$$j(5\tau) = \frac{(t_5^2 + 250t_5 + 3125)^3}{t_5^5}.$$

We can look up an expression for t_5 in terms of t_{25} from [Mai09]:

$$t_5 = t_{25}(t_{25}^4 + 5t_{25}^3 + 15t_{25}^2 + 25t_{25} + 25).$$

We also know that the Fricke involution w_{25} maps t_{25} to $5/t_{25}$. Hence a Hauptmodul for $X_0^+(25)$ is $s := t_{25} + 5/t_{25}$. It follows that

$$j(5\tau) = \frac{((s+5)(s^2-5)(s^2+5s+10))^3}{(s^2+5s+5)^5}.$$

Inserting a K -value for s in this expression yields the j -invariant of an elliptic curve E over K with $H_{E,5} \subseteq V_4$. The condition on $t^2 - 20$ in the statement of the Theorem ensures that we have equality here, by ensuring that the image is not contained in any one of the three subgroups of order 2 in V_4 , as we now demonstrate.

Let E be a curve in $X_s(5)(K)$ corresponding to a choice of s in K . The following statements are readily seen to be equivalent to the previous.

- $H_{E,5}$ is cyclic.
- $G_{E,5}$ is contained in (a conjugate of) C_s^+ .
- E has a pair of distinct K -rational 5-isogenies.
- E pulls back to a K -point on $X_0(25)$.
- $t_{25} \in K$.

Since t_{25} satisfies the polynomial $x^2 - sx + 5$ of discriminant $s^2 - 20$, we have that $t_{25} \in K$ if and only if $s^2 - 20$ is a square in K .

Thus, the statement $s^2 - 20$ is not a square in K is equivalent to $H_{E,5}$ not being cyclic, and hence must be isomorphic to V_4 .

We have, however, overlooked an issue above. For a given $j \in K$, there are at most 15 values of $s \in K$ that yield the same j . This is because the field extension $\mathbb{Q}(s)/\mathbb{Q}(j)$, which has degree 15 and is not Galois, has automorphism group of order at most 15 (and indeed, the number of distinct $s \in K$ yielding j is precisely the size of this automorphism group, which depends on K). We must ensure that for none of the Galois conjugate values is $s^2 - 20$ square in K . This explains the final condition in the statement of the Theorem. \square

To illustrate this theorem, we set $K = \mathbb{Q}(\sqrt{5})$, and input $s = 3\sqrt{5} + 1$ to obtain

$$j = \frac{337876318862280\sqrt{5} + 741305345279328}{41615795893};$$

we check that the other two values of $s \in K$, namely $\frac{\sqrt{5}-15}{7}$ and $\frac{-22\sqrt{5}-30}{19}$, do not satisfy $s^2 - 20$ is a square, and hence this j is indeed exceptional for $\mathbb{Q}(\sqrt{5})$ at 5.

However, if we input $s = \frac{3\sqrt{5}-80}{41}$, we get

$$j = \frac{277374956280053760\sqrt{5} + 622630488102469632}{18658757027251},$$

and whilst $\frac{3\sqrt{5}-80}{41}$ does satisfy $s^2 - 20$ not being a square, this is not the case for $s = 3\sqrt{5} + 2$, which yields the same j -value. One therefore has to be careful of these “pretenders”, hence the last paragraph in the above proof.

We can also insert rational values of s , such as $s = 1$, to obtain elliptic curves over \mathbb{Q} whose basechange to $\mathbb{Q}(\sqrt{5})$ are Hasse at 5, e.g.,

$$j = \frac{-56623104}{161051}.$$

Remark 3.2.3. We have already observed that the local to global principle holds

always at $l = 2$. It also always works at $l = 3$, as a corollary of the group theoretic proposition of the previous section. So $l = 5$ is the smallest Hasse prime.

One might ask for which number fields K there are infinitely many exceptional pairs. Since the modular curves parametrising failures at primes larger than 7 have genus larger than one, and each number field admits only finitely many exceptional primes (by the result of Samuele Anni mentioned in the next section), this question comes down to exceptional pairs for K at 5 and 7. Since we have just analysed 5, and Sutherland has already studied 7, we obtain the following.

Corollary 3.2.4. *A number field K admits infinitely many exceptional pairs if and only if at least one of the following two conditions holds:*

- K contains $\sqrt{5}$;
- The elliptic curve 49a3 has positive rank over K .

3.3 Hasse curves over quadratic fields I: Sutherland-type pairs

We pose the following general task.

Question 3.3.1. *Fix $d \geq 1$. Find all Hasse curves over degree d number fields.*

The $d = 1$ case is dealt with by Sutherland's Theorem 2, as discussed above. In this section, we will consider the $d = 2$ case. We are thus looking for **quadratic Hasse curves**.

We start by reformulating this problem slightly. We consider a pair (K, l) of a quadratic field K and a prime l . Our problem is then equivalent to the following problem.

Question 3.3.2. *For all pairs (K, l) , find all Hasse at l curves over K .*

At this point it is useful to make a distinction between two sorts of pairs; we say that a pair (K, l) is of **Sutherland-type** if $K \neq \mathbb{Q}(\sqrt{l^*})$. In the present section we consider the above problem for Sutherland-type pairs; in the next section we consider the non-Sutherland-type pairs.

In his preprint [Ann13], Samuele Anni has proved the following.

Theorem 3.3.3 (Anni, Theorem 4.3 in [Ann13]). *Let K be a degree d number field, and let E/K be a Hasse at l curve. Then l is contained in the finite set*

$$\{l : l \equiv 3 \pmod{4} \text{ and } l \leq 6d + 1\} \cup \{l : l \equiv 1 \pmod{4} \text{ and } \sqrt{l} \in K\}.$$

Remark 3.3.4. This is almost Theorem 4.3 in *loc. cit.*; there the result is stated under the assumption that $j(E) \notin \{0, 1728\}$. One may remove this assumption with Anni's Lemma 6.1, whose proof shows that, if a Hasse at l curve over a degree d number field has complex multiplication, then l is at most $6d + 1$.

Setting $d = 2$ into this, we find that, if a Sutherland-type pair (K, l) admits a Hasse curve, then $l = 7$ or 11 .

We are now reduced to finding Sutherland-type pairs of the form $(K, 7)$ and $(K, 11)$.

The first of these is easy to determine; any Hasse at 7 curve over K corresponds to a K -point on the elliptic curve 49a3; these can be determined.

What about the latter question, that of Hasse at 11 curves over quadratic fields K ? We believe that these do not exist.

Conjecture 3.3.5. *There are no quadratic Hasse at 11 curves.*

To explain our motivation for making this conjecture, we begin with the following result.

Proposition 3.3.6. *There are only finitely many quadratic Hasse at 11 curves.*

Proof. By Sutherland's group theoretic result, a quadratic Hasse at 11 curve is characterised by $H_{E,11} \cong D_{10}$, and hence yields a quadratic point on the modular curve $X_{D_{10}}(11)$ classifying elliptic curves with $H_{E,11} \subseteq D_{10}$. We now relate this modular curve to a more usual one.

Lemma 3.3.7. *$X_{D_{10}}(11)$ is defined over \mathbb{Q} . It is the $\mathbb{Q}(\sqrt{-11})$ -twist of the modular curve $X_0(121)$.*

Proof. That $X_{D_{10}}(11)$ is defined over \mathbb{Q} follows from the pullback $\pi^{-1}(D_{10})$ of D_{10} to $\mathrm{GL}_2(\mathbb{F}_{11})$ having surjective determinant. Over $\overline{\mathbb{Q}}$, we can see that $X_{D_{10}}(11)$ and $X_0(121)$ are isomorphic by observing that $\pi^{-1}(D_{10}) \cap \mathrm{SL}_2(\mathbb{F}_{11})$ is conjugate to the group of diagonal matrices in $\mathrm{SL}_2(\mathbb{F}_{11})$; thus the two curves are isomorphic over some extension of \mathbb{Q} , which we now show is $\mathbb{Q}(\sqrt{-11})$. A $\mathbb{Q}(\sqrt{-11})$ -point of $X_{D_{10}}(11)$ corresponds to an elliptic curve E over $\mathbb{Q}(\sqrt{-11})$ whose $H_{E,11} \subseteq D_{10} \cap \mathrm{PSL}_2(\mathbb{F}_{11}) \cong C_5$, and hence $G_{E,11}$ is contained in a Cartan subgroup, which must be split; that is, the two curves represent the same moduli problem over $\mathbb{Q}(\sqrt{-11})$. \square

It follows from this identification of the geometry of these modular curves that $X_{D_{10}}(11)$ is neither hyperelliptic nor bielliptic (that is, it does not admit a map of degree at most 2 to a curve of genus at most 1). See [Bar13] for the result that $X_0(121)$ is neither hyperelliptic nor bielliptic.

The claim of the proposition now follows from a theorem of Harris and Silverman ([HS91]) which ensures finitely many quadratic points on such curves. \square

We now describe a method which, given a specific quadratic field K , can find the Hasse at 11 curves over K , if any. As Sutherland showed, a Hasse at 11 curve over K arises as a K -point on the genus 2 modular curve $X_s(11)$, which may be given the following model over \mathbb{Q} :

$$Y^2 = 4X^6 - 4X^4 - 2X^3 + 2X^2 + \frac{3}{2}X + \frac{1}{4}$$

The j -invariants of the corresponding elliptic curves may be computed in a similar fashion to that described in the next chapter. Having now obtained a finite list of values of j as elements of K , we would like to know whether any of the corresponding elliptic curves have $H_{E,11} \cong D_{10}$ (a priori $H_{E,11}$ will be a subgroup of D_{20}). For this, we may apply a recent algorithm of Sutherland, which computes the mod- l Galois image of any elliptic curve over any number field. We may then run this algorithm for every quadratic field whose discriminant is within a given bound.

We did this for every quadratic field whose discriminant D is bounded by 10^4 . We did not determine provably the K -points on $X_s(11)$ for each K , we merely searched for K -points up to height 10^6 in the interest of speed (however, Magma does have support for determining quadratic points on hyperelliptic curves). This yielded 122 quadratic values, and we asked Andrew Sutherland to compute the projective mod-11 Galois image for each of these; in every single case we had $H_{E,11} \cong D_{20}$. We record this in the following result.

Proposition 3.3.8. *Let K be a quadratic field with absolute discriminant bounded by 10^4 , and $P \in X_s(11)(K)$ a point of height less than 10^6 . Then for every elliptic curve E over K with $j(E) = j(P)$, we have $H_{E,11} \cong D_{20}$, and in particular, E is not Hasse at 11.*

If we had an effective version of the result of Harris and Silverman, to the extent of being able to find an upper bound on the absolute value of the discriminant of those quadratic fields K for which $X_s(11)$ has K -points, then we may run our algorithm up to this bound; we would either prove our conjecture, or find a counterexample.

Question 3.3.9. *What is the smallest degree number field over which we have a Hasse at 11 curve? Is there one at degree 3?*

3.4 Hasse curves over quadratic fields II: non Sutherland type pairs

In this section we consider Hasse curves attached to non-Sutherland-type pairs, which must therefore be $(\mathbb{Q}(\sqrt{l^*}), l)$; we denote this pair by P_l . If $l \equiv 3 \pmod{4}$, then P_l does not admit Hasse curves, so henceforth assume $l \equiv 1 \pmod{4}$. Such a pair may admit two sorts of Hasse curve: **exceptional Hasse curves** (where the projective mod- l image is isomorphic to A_4 , A_5 or S_4) and **dihedral Hasse curves** (where the projective mod- l image is dihedral). We consider each in turn.

Proposition 3.4.1. *An exceptional quadratic Hasse curve can only occur at the prime 13, over $\mathbb{Q}(\sqrt{13})$, where it has projective A_4 -image. Conversely, such a curve is a quadratic Hasse curve.*

Proof. Let K be a quadratic field. If E/K is exceptional Hasse at l , then $K = \mathbb{Q}(\sqrt{l^*})$, and $l \equiv 1 \pmod{12, 24 \text{ or } 60}$, according as the projective image be A_4 , S_4 or A_5 . However, there is the following general fact regarding the projective mod- p image, and we are grateful to **Nicolas Billerey** for bringing it to our attention; for F a number field, and p a prime, let

$$e_p := \max_{\mathfrak{p}} \{e_{\mathfrak{p}}\},$$

where $e_{\mathfrak{p}}$ denotes the ramification index of the prime $\mathfrak{p}|p$.

Fact 3.4.2 (Agnès David, Lemme 2.5 in [Dav11]). *For an elliptic curve over a number field F , the projective mod- p image must contain an element of order $\frac{p-1}{4e_p}$.*

Applying this lemma in our case, we get that

- A_4 can occur as $H_{E,l}$ only if $l < 25$;
- S_4 can occur as $H_{E,l}$ only if $l < 33$;

- A_5 can occur as $H_{E,l}$ only if $l < 41$.

But we also know that

- A_4 is Hasse only if $l \equiv 1 \pmod{12}$;
- S_4 is Hasse only if $l \equiv 1 \pmod{24}$;
- A_5 is Hasse only if $l \equiv 1 \pmod{60}$.

Putting these conditions together, we obtain the forward implication of the proposition. The converse has already been proven in 3.1.4. \square

The following question is now very natural.

Question 3.4.3. *Let $K = \mathbb{Q}(\sqrt{13})$. Does there exist an elliptic curve E/K whose projective mod-13 representation is isomorphic to A_4 ?*

Such a curve must be Hasse at 13; it will also *not* have an isogeny over a quadratic extension, as the dihedral failures must have; rather one must go up to a degree 4 extension before we get a rational isogeny. Answering this question will be the subject of Chapters 4 and 5.

We now consider the dihedral Hasse curves:

Question 3.4.4. *For each $l \equiv 1 \pmod{4}$, find the elliptic curves E over $\mathbb{Q}(\sqrt{l})$ whose $H_{E,l} \cong D_{2n}$ for some $1 < n \mid \frac{l-1}{2}$.*

We have not been able to resolve this question except in the case $l = 5$ (see Section 3.2). We can say that, for all other l , there are only finitely many such curves, as the genus of the corresponding modular curve will be larger than 1.

A positive answer to the **Strong Serre Uniformity Problem** would imply that there are only finitely many l for which such dihedral elliptic curves exist. Let us explain this further.

In his book [Ser68], Serre proved what is known as the **Open Image Theorem**; it implies, given a non-CM elliptic curve E over a number field K , that there is a bound $c(E, K)$, depending on both E and K , such that, if l is a prime larger than $c(E, K)$, then the mod- l Galois image $G_{E,l}$ attached to E is all of $\mathrm{GL}_2(\mathbb{F}_l)$.

A few years later, in his paper [Ser72], Serre asked if the constant $c(E, K)$ could be made independent of E : does there exist a bound $c(K)$ such that, for every elliptic curve E over K , and any prime $l > c(K)$, we have $G_{E,l} = \mathrm{GL}_2(\mathbb{F}_l)$? This problem is known as the Serre Uniformity Problem. It is not known for a single number field.

The **Strong Serre Uniformity Problem** asks further for the bound $c(K)$ to depend only on the degree of K : does there exist a bound $c(d)$ such that, for any elliptic curve E over any number field of degree at most d , we have $G_{E,l} = \mathrm{GL}_2(\mathbb{F}_l)$?

Assuming that this stronger problem has an affirmative answer for $d = 2$, we see that dihedral quadratic Hasse at l curves must have CM for sufficiently large l . However, by the work of Anni mentioned in the previous section (3.3.4), Hasse curves do not have CM for l sufficiently large, so in fact there should only be finitely many primes l for which there exist quadratic dihedral Hasse curves.

Actually determining these may be approached by studying $\mathbb{Q}(\sqrt{l})$ -points on the modular curve $X_s(l)$, which is a difficult problem.

3.5 Fields admitting no exceptional pairs

We say that a number field is **special** if it admits no Hasse curves. Every odd degree field is not special, because Sutherland's Hasse at 7 curve, when base changed to the number field, is still Hasse at 7. Thus, special fields must have even degree; more precisely, special fields must contain $\sqrt{-7}$.

Question 3.5.1. *What are the special number fields for each even degree?*

Proposition 3.5.2. *The only special quadratic field is $\mathbb{Q}(\sqrt{-7})$.*

Proof. Over every other quadratic field, Sutherland's Hasse curve is still Hasse. Over $\mathbb{Q}(\sqrt{-7})$, 7 is not allowed to be a Hasse prime, since it is not congruent to 1 mod 4. The result of Samuele Anni of the previous section says that the only other Hasse prime to consider is 11. As in the previous section, we may check, for a given quadratic field K , the Hasse at 11 curves over K , and verify that there are none for $K = \mathbb{Q}(\sqrt{-7})$. \square

The following is a natural question which we do not address in this thesis.

Question 3.5.3. *What about degree 4 special fields?*

3.6 From almost all to all

Recall that, in our motivating question 2.2.4, we ask if **almost all** reductions having an l -isogeny implies the elliptic curve itself has an l -isogeny, and we have seen that most¹ curves do have this property. Specifically, we excluded the primes of bad reduction, as well as the primes dividing l .

One may, however, ask an *a priori* more demanding question. It is clear that, for \mathfrak{p} a prime of good reduction, not dividing l , we have

$$\tilde{E}_{\mathfrak{p}} \text{ has } \mathbb{F}_{\mathfrak{p}}\text{-rational } l\text{-isogeny} \iff E/K_{\mathfrak{p}} \text{ has } K_{\mathfrak{p}}\text{-rational } l\text{-isogeny}.$$

But now the right hand side makes sense for all \mathfrak{p} ; thus, we could ask:

Question 3.6.1 (Stronger local to global problem for isogenies). *If E/K has a $K_{\mathfrak{p}}$ -rational l -isogeny for all \mathfrak{p} , then must it have a K -rational one?*

Similarly to before, we say that an elliptic curve E/K is **strongly Hasse at l** if the answer to this question for E is no.

¹We mean that curves failing this property correspond to rational points on modular curves, which we expect to be “rare”.

Clearly, if E is strongly Hasse at l , then it is Hasse at l . But do strong Hasse curves even exist? Yes they do.

Proposition 3.6.2. *There exist elliptic curves E over number fields K which do not admit a K -rational l -isogeny for a prime l , but do admit $K_{\mathfrak{p}}$ -rational l -isogeny for all primes \mathfrak{p} of K .*

This follows from the following proposition.

Proposition 3.6.3. *If E/K is Hasse at l , then a finite computation determines whether or not E is strongly Hasse at l .*

In the following proof, $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$ denotes the classical Modular Polynomial at N .

Proof. Let E/K be Hasse at l . We need to determine, for each $\mathfrak{p} \in S$, whether or not $E/K_{\mathfrak{p}}$ has $K_{\mathfrak{p}}$ -rational l -isogeny. By a theorem of Igusa ([Igu59]), this is equivalent to asking whether or not the polynomial $\Phi_l(X, j_E)$ has a root in $K_{\mathfrak{p}}$. By Hensel's Lemma, this reduces to a finite computation. \square

Example 3.6.4. Let us answer the above question for $K = \mathbb{Q}$. Here we know that Sutherland's j -invariant $\frac{2268945}{128}$ is the only Hasse j -invariant. Sutherland in fact shows that, modulo every odd prime, the polynomial $\Phi_7(X, \frac{2268945}{128}) \in \mathbb{Q}[X]$ has a linear factor, though not over \mathbb{Q} . So, for the present question, we are only asking whether or not this polynomial has a linear factor when viewed over \mathbb{Q}_2 . We checked this in Magma, and it turns out that it does indeed have a linear factor. That is, *there is a unique rational elliptic curve failing the stronger local to global principle for isogenies*, and it is the same as Sutherland's Hasse at 7 curve.

Example 3.6.5. We show in the next chapter that the pairs

$$(13, \frac{\pm 18171572224000\sqrt{13} + 65520558080000}{1594323})$$

are exceptional for $\mathbb{Q}(\sqrt{13})$. Again using Magma to carry out the aforementioned finite computation reveals that this elliptic curve is also strongly Hasse at 13.

Based upon these two example alone, one may hope that the answer to the following question is “Yes”.

Question 3.6.6. *If E/K is Hasse at l , is it necessarily strongly Hasse?*

We are not, however, so convinced as to state this as a conjecture.

We end this section by recasting this stronger question into a form that more closely resembles the **Hasse principle for varieties**. If X/K is a projective smooth variety over a number field K , we define the **adelic points of X** , denoted $X(\mathbb{A}_K)$, to be the set

$$X(\mathbb{A}_K) := \prod_{\mathfrak{p}} X(K_{\mathfrak{p}}).$$

We have a diagonal embedding

$$X(K) \rightarrow X(\mathbb{A}_K);$$

thus, if X possesses a K -point, then it admits an adelic point. The Hasse Principle for varieties would say the converse: if X admits an adelic point, then it must admit a rational point. This is not true for every variety (so perhaps the use of “principle” is not warranted), though there is much current research aimed at understanding the obstruction to this, depending on the nature of the variety X .

The above question may be cast into this framework, by using the modular curve $X_0(l)$. Consider the following commutative diagram:

$$\begin{array}{ccc} X_0(l)(K) & \longrightarrow & X_0(l)(\mathbb{A}_K) \\ j \downarrow & & \downarrow \Pi j \\ X_0(1)(K) & \xrightarrow{\phi} & X_0(1)(\mathbb{A}_K) \end{array}$$

We say an adelic point $P \in X_0(l)(\mathbb{A}_K)$ is **isotrivial** if its image under $\prod j$ is in the image of ϕ . The following is now a clear consequence of the definitions.

Proposition 3.6.7. *The stronger local to global problem for degree l isogenies is equivalent to asking if every isotrivial adelic point on $X_0(l)$ comes from a K -rational point.*

3.7 Hasse surfaces

In the final section of this chapter we consider Hasse varieties of dimension 2, which we refer to as **Hasse surfaces**. Following Sutherland's approach, we first need to determine which subgroups of $\mathrm{PGSp}_4(\mathbb{F}_l)$, for prime l , are Hasse, and second we need to construct abelian surfaces A whose $H_{A,l}$ is one of the Hasse subgroups we identified.

The first part of this approach has recently been carried out by John Cullinan [Cul12]. Given a subgroup $H \subseteq \mathrm{PGSp}_4(\mathbb{F}_l)$, let $\pi^{-1}(H)$ denote the pullback of H to $\mathrm{GSp}_4(\mathbb{F}_l)$.

Theorem 3.7.1 (Cullinan). *A subgroup $H \subseteq \mathrm{PGSp}_4(\mathbb{F}_l)$ is Hasse if and only if $\pi^{-1} \cap \mathrm{Sp}_4(\mathbb{F}_l)$ is isomorphic to one of the following groups.*

Group	Condition
C_s^+	$l \equiv 1(4)$
$(l-1)/2 \cdot \mathrm{SL}_2(\mathbb{F}_3) \cdot 2$	$l \equiv 1(24)$
$(l-1)/2 \cdot \mathrm{GL}_2(\mathbb{F}_3) \cdot 2$	$l \equiv 1(24)$
$(l-1)/2 \cdot \widehat{S}_4 \cdot 2$	$l \equiv 1(24)$
$(l-1)/2 \cdot \mathrm{SL}_2(\mathbb{F}_5) \cdot 2$	$l \equiv 1(60)$
$D_{(l-1)/2} \wr S_2$	
$\mathrm{SL}_2(\mathbb{F}_3) \wr S_2$	$l \equiv 1(48)$
$\widehat{S}_4 \wr S_2$	$l \equiv 1(48)$
$\mathrm{SL}_2(\mathbb{F}_5) \wr S_2$	$l \equiv 1(12)$
$2_-^{1+4} \cdot O_4^-(2)$	$l \equiv 1(12)$
$2_-^{1+4} \cdot 3$	$l \equiv 5(24)$
$2_-^{1+4} \cdot 5$	$l \equiv 5(40)$
$2_-^{1+4} \cdot S_3$	$l \equiv 5(24)$
$2 \cdot S_6$	$l \equiv 1(12)$
$\mathrm{SL}_2(\mathbb{F}_5)$	$l \equiv 1(30)$
$\mathrm{SL}_2(\mathbb{F}_3)$	$l \equiv 1(24)$

(We refer to *loc. cit.* for the group-theoretic notation used in the above table.)

At this point we may artificially engineer Hasse surfaces over arbitrary number fields. For example, suppose we would like to construct an abelian surface A whose $G_{A,l} \cap \mathrm{Sp}_4(\mathbb{F}_l)$ is isomorphic to $\mathrm{SL}_2(\mathbb{F}_5)$ for some prime $l \equiv 1 \pmod{30}$; by the above table, this would give a Hasse surface. We first take an abelian surface over \mathbb{Q} with trivial absolute endomorphism ring. Serre's Open Image Theorem, which holds also for abelian surfaces (see [Hal11]), ensures that, for all sufficiently large primes l , we have $G_{A,l} \cong \mathrm{GSp}_4(\mathbb{F}_l)$. Choose such a sufficiently large l which is also congruent to $1 \pmod{30}$. We then base-change A to force the new $G_{A,l}$ to satisfy $G_{A,l} \cap \mathrm{Sp}_4(\mathbb{F}_l)$ to be isomorphic to $\mathrm{SL}_2(\mathbb{F}_5)$, using the Galois correspondence.

However, a more honest challenge is to find Hasse surfaces *over* \mathbb{Q} , pre-empting this base-change cheat.

Proposition 3.7.2. *Hasse surfaces over \mathbb{Q} exist.*

Indeed, let E/\mathbb{Q} be the Hasse at 7 elliptic curve found by Sutherland, let G be its mod 7 Galois image, and consider E^2 . Its mod 7 Galois image is isomorphic to

$$\left\{ \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix} : A \in G \right\} \subset \mathrm{GSp}_4(\mathbb{F}_7),$$

which is a Hasse subgroup of $\mathrm{GSp}_4(\mathbb{F}_7)$ (see the proof of Lemma 3.7.5 and Remark 3.7.6). Thus, E^2 is a Hasse at 7 surface over \mathbb{Q} .

The following question is then natural.

Question 3.7.3. *Do there exist simple Hasse surfaces over \mathbb{Q} ?*

Either answer to this question would be interesting. There do exist moduli spaces of abelian surfaces with level structure; these spaces have dimension 3 as varieties, and compared to the moduli of elliptic curves are far less-well understood. Perhaps one may find examples of simple Hasse surfaces over \mathbb{Q} by constructing \mathbb{Q} -points on a suitable moduli space.

Restricting the class of simple abelian surfaces somehow may make the above question more tractable. For example, consider the class of *modular abelian surfaces over \mathbb{Q}* ; these are the abelian surfaces A_f attached to weight 2 newforms f whose Fourier coefficient field K_f is a quadratic number field. More generally, if K_f is a number field of degree d , then A_f will be an abelian variety of dimension d ; we refer to A_f in this case as a *modular abelian variety*. It is a theorem of Ribet that these abelian varieties are simple over \mathbb{Q} (see for example [Rib76]).

Question 3.7.4. *Does there exist a Hasse modular abelian variety A_f ?*

These varieties have the important property of having GL_2 -type: the l -adic Tate module, for each l , splits as a direct sum

$$T_l A_f = \bigoplus_{\lambda|l} T_{f,\lambda},$$

where each $T_{f,\lambda}$ is a free module of rank 2 over the λ -adic completion $\mathbb{Z}_{f,\lambda}$ of the ring of integers \mathbb{Z}_f of K_f . This formula allows us to consider the $2d$ -dimensional l -adic Galois representation $T_l A_f$ as a sum of 2-dimensional λ -adic representations; these 2-dimensional representations are, by definition, the λ -adic Galois representations attached to f (see Chapter 9, Section 5 of [DS05]).

Consider the special case of $d = 2$ and l splitting in \mathbb{Z}_f . By taking the reduction modulo l of the above formula, we obtain a splitting

$$A_f[l] = V_{f,\lambda} \oplus V_{f,\lambda'}$$

of the 4-dimensional $G_{\mathbb{Q}}$ -representation $A_f[l]$ as a sum of two 2-dimensional representations. Thus, $G_{A_f,l}$ is contained in the sum of two subgroups H, H' of $\mathrm{GL}_2(\mathbb{F}_l)$:

$$G_{A_f,l} \subseteq \begin{pmatrix} H & 0 \\ 0 & H' \end{pmatrix}.$$

We choose H and H' *minimally*; i.e., H is the image of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acting on $V_{f,\lambda}$, and H' the image of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acting on $V_{f,\lambda'}$.

Lemma 3.7.5. *If one of $\{H, H'\}$ is Hasse, and the other is not contained in a Borel subgroup, then A_f is Hasse.*

Proof. We first show that $G_{A_f,l}$ does not fix a line in $A_f[l]$. If it did, then one of H or H' must fix a line in $V_{f,\lambda}$, respectively $V_{f,\lambda'}$, which is not allowed under the hypotheses on $\{H, H'\}$.

Without loss of generality we suppose that H is Hasse. Each element of $G_{A_f,l}$ may be written as $y = \begin{pmatrix} h & 0 \\ 0 & h' \end{pmatrix}$ for $h \in H$, $h' \in H'$. Since h fixes a line in $V_{f,\lambda}$, y fixes the same line; thus, every element of $G_{A_f,l}$ fixes a line, and the proof is complete. \square

Remark 3.7.6. The above proof works for any abelian surface whose mod l Galois image is contained in $\begin{pmatrix} H & 0 \\ 0 & H' \end{pmatrix}$ for subgroups H, H' of $\text{GL}_2(\mathbb{F}_l)$.

We summarise the above discussion in the following proposition; it expresses a sufficient condition for our A_f to be Hasse.

Proposition 3.7.7. *Let f be a weight 2 newform with quadratic Fourier coefficient field K_f , and l a prime which splits in K_f as $(l) = \lambda\lambda'$. Let H be the image in $\text{GL}_2(\mathbb{F}_l)$ of $\bar{\rho}_{f,\lambda}$, and H' the image of $\bar{\rho}_{f,\lambda'}$. If one of $\{H, H'\}$ is Hasse, and the other is not contained in a Borel subgroup, then the modular abelian surface A_f is Hasse.*

We have not been able to find an f satisfying the conditions of the above proposition. We have also not yet fully understood the case of l being inert in K_f .

Chapter 4

The Hunt for Tetrahedral at 13 Elliptic Curves

In the last chapter, when studying quadratic Hasse curves, we encountered the following question.

Question 4.0.8. *Does there exist an elliptic curve over $\mathbb{Q}(\sqrt{13})$ whose projective mod-13 image is isomorphic to A_4 ?*

The main result of this chapter is the following.

Theorem 4.0.9. *The answer is “Yes”. Indeed, the elliptic curves over \mathbb{Q} with j -invariant*

$$\frac{11225615440}{1594323}, -\frac{160855552000}{1594323}, \frac{90616364985637924505590372621162077487104}{197650497353702094308570556640625}$$

have projective mod-13 image isomorphic to S_4 ; thus, when base-changed to $\mathbb{Q}(\sqrt{13})$, they have projective mod-13 image isomorphic to A_4 . We even have an example that is not a base change; any elliptic curve over $\mathbb{Q}(\sqrt{13})$ with j -invariant equal to

$$j = \frac{\pm 18171572224000\sqrt{13} + 65520558080000}{1594323}$$

has projective mod-13 image isomorphic to A_4 .

The approach we take is to consider the modular curve parametrising these desired curves, and to find an explicit model for it.

4.1 $X_{S_4}(l)$ and $X_{A_4}(l)$

Let $l \geq 5$ be a prime. By Theorem 4.2 (1) of [Bea10], the group $\mathrm{PGL}_2(\mathbb{F}_l)$ has a unique (up to conjugacy) subgroup isomorphic to S_4 , and similarly for A_4 . Consider the pullback to $\mathrm{GL}_2(\mathbb{F}_l)$ of these subgroups, and denote the corresponding modular curves by $X_{S_4}(l)$ and $X_{A_4}(l)$. Points on these curves thus correspond to elliptic curves E with $H_{E,l}$ being contained in a conjugate of S_4 , respectively A_4 .

Lemma 4.1.1. • $X_{A_4}(l)$ is defined over $\mathbb{Q}(\sqrt{l^*})$.

- $X_{S_4}(l)$ is defined over \mathbb{Q} if and only if $l \equiv 3$ or $5 \pmod{8}$, and is defined over $\mathbb{Q}(\sqrt{l^*})$ otherwise.

Proof. For all $l \geq 5$, A_4 is in fact contained in $\mathrm{PSL}_2(\mathbb{F}_l) \subset \mathrm{PGL}_2(\mathbb{F}_l)$ (recall 3.1.3). Thus, the image of the determinant map on the pullback of A_4 to $\mathrm{GL}_2(\mathbb{F}_l)$ is precisely the squares in \mathbb{F}_l^* , and so the field denoted $M_{G,l}$ in 2.4 is $\mathbb{Q}(\sqrt{l^*})$. The case of S_4 is similar. \square

Proposition 4.1.2. *If $l \equiv 3$ or $5 \pmod{8}$, then $X_{A_4}(l) = X_{S_4}(l)_{\mathbb{Q}(\sqrt{l^*})}$.*

Proof. The two curves are isomorphic over $\overline{\mathbb{Q}}$, and there is an obvious nonconstant map between the two curves defined over $\mathbb{Q}(\sqrt{l^*})$, so they must be isomorphic as curves over $\mathbb{Q}(\sqrt{l^*})$. \square

Therefore, when $l \equiv 3$ or $5 \pmod{8}$, both of these two curves, when viewed over the complex numbers \mathbb{C} , have the description

$$\Gamma_{A_4}(l) \backslash \mathcal{H}^*,$$

where $\Gamma_{A_4}(l)$ means the pullback to $\mathrm{PSL}_2(\mathbb{Z})$ of $A_4 \subset \mathrm{PSL}_2(\mathbb{F}_l)$.

Remark 4.1.3. If $l \equiv 1$ or $7 \pmod{8}$, and $l > 7$, then the two curves $X_{S_4}(l)$ and $X_{A_4}(l)$, both defined over $\mathbb{Q}(\sqrt{l^*})$, are *not* isomorphic over \mathbb{C} since, as one may check, they have different genera. We do however still have a rational map

$$X_{A_4}(l) \longrightarrow X_{S_4}(l).$$

The following is an application of the explicit formula for the genus of modular curves given in 2.4.

Proposition 4.1.4. *If $l \equiv 3$ or $5 \pmod{8}$, then*

$$\mathrm{genus}(X_{A_4}(l)) = \mathrm{genus}(X_{S_4}(l)) = 1 + \frac{\mu_l}{12} - \frac{e_{2,l}}{4} - \frac{e_{3,l}}{3} - \frac{e_{\infty,l}}{2},$$

where

- $\mu_l = \frac{1}{24}l(l^2 - 1)$;
- $e_{2,l} = \frac{l \pm 1}{4}$;
- $e_{3,l} = \frac{l \pm 1}{3}$;
- $e_{\infty,l} = \frac{l^2 - 1}{24}$.

(In each case, take the sign that makes the quantity integral.)

For example, taking $l = 13$, we find that $X_{S_4}(13)$ has genus 3.

By the above results, the motivating question for this chapter can be answered by determining the $\mathbb{Q}(\sqrt{13})$ -points on the curve $X_{S_4}(13)$. For this reason, we would like to **write down an explicit equation for this curve**. There is a general strategy for doing this; in the next section we sketch this strategy and carry it out.

4.2 The equation for $X_{S_4}(13)$

In *Equations for Modular Curves* [Gal96], Steven Galbraith gives an algorithm for writing down equations for modular curves of various kinds (though he is chiefly interested in the cases $H = \text{Borel}$ and $\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$, corresponding to $X_0(l)$ and $X_1(l)$).

We review his algorithm in the case where the modular curve has genus 3.

Step 1. Write down the q -expansion up to some precision of a basis of the \mathbb{C} -vector space $S_2(\Gamma_H(l))$; call these basis forms X, Y, Z .

Step 2. Consider the degree 2 monomials in X, Y, Z , and search for a linear relation among these monomials, up to the precision.

Step 3. If a relation is found, then the modular curve being considered is hyperelliptic; see Chapter 4 of *loc. cit.* for more on obtaining a model in this case. If no relation is found, then the curve is not hyperelliptic; repeat Step 2, replacing “degree 2” with “degree 4”. One is bound to find a relation, and this equation will be the equation for the curve.

The point is that, if we can do Step 1, then the rest is just linear algebra. However, carrying out Step 1 for our curve $X_{S_4}(13)$ is not at all a trivial matter, and in fact demands a whole chapter of explanation. Thus, in the next chapter we will prove the following result, whilst in the current chapter we will use it to obtain our goal.

Theorem 4.2.1. *Let $\zeta := e^{2\pi i/13}$, $q := e^{2\pi iz/13}$, and $\mathbb{Q}(\zeta)$ the corresponding cyclotomic field. A basis of $S_2(\Gamma_{A_4}(13))$ is given by $\{f, g, h\}$, with*

$$\begin{aligned} f &= -q + (-\zeta^{11} - \zeta^{10} - \zeta^3 - \zeta^2)q^2 + (\zeta^{11} + \zeta^{10} - \zeta^9 - \zeta^7 - \zeta^6 - \zeta^4 + \zeta^3 + \zeta^2 - 2)q^3 + \dots \\ g &= (-\zeta^{11} - \zeta^{10} - \zeta^9 - \zeta^7 - \zeta^6 - \zeta^4 - \zeta^3 - \zeta^2 - 1)q + (-\zeta^{11} - \zeta^{10} - \zeta^9 - \zeta^7 - \zeta^6 - \zeta^4 - \zeta^3 - \zeta^2 - 2)q^2 + \\ &\quad (-\zeta^{11} - \zeta^{10} - \zeta^3 - \zeta^2 - 1)q^3 + \dots \\ h &= (\zeta^{11} + \zeta^{10} + \zeta^3 + \zeta^2 + 3)q + (-\zeta^{11} - \zeta^{10} - \zeta^9 - \zeta^7 - \zeta^6 - \zeta^4 - \zeta^3 - \zeta^2 - 3)q^2 + q^3 + \dots \end{aligned}$$

The precision can be made arbitrarily high. In fact, the coefficients all lie in the

unique cubic subfield of $\mathbb{Q}(\zeta)$.

Carrying out Step 2 yields no linear relation among the degree 2 monomials in these basis forms, so we proceed to Step 3; we consider the degree 4 monomials in $\{f, g, h\}$, explicitly as q -expansions, and search for a linear relation among them. In this way we obtain the following result.

Theorem 4.2.2. *The modular curve $X_{S_4}(13)$ has the model*

$$\begin{aligned} \mathcal{C} : 4X^3Y - 3X^2Y^2 + 3XY^3 - X^3Z + 16X^2YZ - 11XY^2Z + \\ 5Y^3Z + 3X^2Z^2 + 9XYZ^2 + Y^2Z^2 + XZ^3 + 2YZ^3 = 0, \end{aligned}$$

considered as a smooth projective curve inside $\mathbb{P}_{\mathbb{Q}}^2$.

4.3 Obtaining octahedral elliptic curves over \mathbb{Q}

In this section we obtain the main theorem of the chapter.

4.3.1 Step 1. Compute the j -map

Here we explicitly determine the j -map

$$X_{S_4}(13) \xrightarrow{j} X(1) \cong \mathbb{P}_{\mathbb{Q}}^1$$

as a rational function on $X_{S_4}(13)$. This is a function of degree 91, which we seek to express in the form

$$j(X, Y, Z) = \frac{n(X, Y, Z)}{d(X, Y, Z)},$$

where n and d are polynomials of the same degree over \mathbb{Q} . We first find a suitable denominator $d(X, Y, Z)$. The poles of j are all of order 13 and are at the 7 cusps

of $X_{S_4}(13)$, so we will find these, as $\overline{\mathbb{Q}}$ -rational points on $X_{S_4}(13)$. Then we find a cubic in $\mathbb{Q}[X, Y, Z]$ which passes through these 7 points (there is no quadratic which does), and the 13th power of this cubic is the denominator d . Having found d we determine the numerator n using linear algebra on q -expansions.

Remark 4.3.1. It would also be possible, in principal, to follow [Bar12a] by computing the zeros of j numerically to sufficient precision to be able to recognise them as algebraic points, as then we would have the full divisor of the function j from which j itself could be recovered using an explicit Riemann-Roch space computation. Our method has the advantage of not requiring any numerical approximations.

We first need to find which points on our model \mathcal{C} for $X_{S_4}(13)$ are the 7 cusps. It turns out that there are three which are defined and conjugate over the degree 3 subfield $\mathbb{Q}(\alpha)$ of $\mathbb{Q}(\zeta)$, where $\zeta = \zeta_{13}$ and $\alpha = \zeta + \zeta^5 + \zeta^8 + \zeta^{12}$, and the other four are defined and conjugate over the degree 4 subfield $\mathbb{Q}(\beta)$ of $\mathbb{Q}(\zeta)$, where $\beta = \zeta + \zeta^3 + \zeta^9$.

Proposition 4.3.2. *On the model \mathcal{C} for $X_{S_4}(13)$, the 7 cusps are given by the three Galois conjugates of*

$$[-3\alpha^2 - 7\alpha + 1 : 4\alpha^2 + 11\alpha - 3 : 5]$$

and the four conjugates of

$$[3\beta^3 + 6\beta^2 + 6\beta - 15 : \beta^3 + \beta^2 - 4\beta - 4 : 9],$$

where α and β have minimal polynomials $x^3 + x^2 - 4x + 1$ and $x^4 + x^3 + 2x^2 - 4x + 3$ respectively.

The degree 3 cusps are easy to obtain; the cusp corresponding to the point $i\infty$ on the extended upper half-plane \mathcal{H}^* has coordinates given by the leading coefficients

of the three basis cuspforms f, g, h ; denoting by φ the map

$$\begin{aligned}\varphi : \Gamma_{A_4}(13) \backslash \mathcal{H}^* &\xrightarrow{\sim} X_{S_4}(13) \\ \Gamma_{A_4}(13) \cdot z &\longmapsto [f(z) : g(z) : h(z)],\end{aligned}$$

we see that $\varphi(i\infty) = [a_1(f) : a_1(g) : a_1(h)]$. Expressing these coordinates in terms of α gives the degree 3 cusp given in the proposition.

It is possible to determine in advance the Galois action on the cusps, as in the following Lemma. However, note that in practice our method to compute the cusps algebraically, given below, does not require this knowledge in advance.

Lemma 4.3.3. *The absolute Galois group of \mathbb{Q} acts on the seven cusps with two orbits, of sizes 3 and 4.*

Proof. We know *a priori* that the cusps are all defined over $\mathbb{Q}(\zeta_{13})$. Theorem 1.3.1 in [Ste82] explains how to compute the action of $\text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^*$ on the cusps of a modular curve X of level N , provided that the field of rational functions on X is generated by rational functions whose q -expansions have rational coefficients. This does not apply here, since the field of modular functions for $\Gamma_{A_4}(13)$ is not generated by functions with rational q -expansions, but rather by functions with q -expansions in the cubic field $\mathbb{Q}(\alpha)$. But following Stevens' method we can compute the action of the absolute Galois group of $\mathbb{Q}(\alpha)$, which acts through the cyclic subgroup of order 4 of $(\mathbb{Z}/13\mathbb{Z})^*$ fixing α . We find that it fixes three cusps (which we already know from above, as they are defined over $\mathbb{Q}(\alpha)$), and permutes the remaining four cyclically. It follows that the other four cusps are also permuted cyclically by the full Galois group, and hence have degree 4 as claimed. \square

It remains to find the coordinates of one cusp of degree 4.

Let $c \in \Gamma_{A_4}(13) \backslash \mathbb{P}^1(\mathbb{Q})$ be any cusp. Then there exists $\gamma \in \text{PSL}_2(\mathbb{Z}) \backslash \Gamma_{A_4}(13)$

such that $\gamma(c) = \infty$, and hence,

$$\alpha(c) = [a_1(f|\gamma) : a_1(g|\gamma) : a_1(h|\gamma)].$$

In the next chapter we will explain how to compute the action of $\mathrm{PSL}_2(\mathbb{Z})$ on the cuspforms f, g, h ; therefore, we can compute the right-hand side of the above equation for any γ . We choose random $\gamma \in \mathrm{PSL}_2(\mathbb{Z})$ until we find a point which is not one of the three conjugates we already have. This proves the above proposition.

Next we find a cubic curve passing through these 7 points.

Proposition 4.3.4. *The following cubic passes through the seven cusps:*

$$5X^3 - 19X^2Y - 6XY^2 + 9Y^3 + X^2Z - 23XYZ - 16Y^2Z + 8XZ^2 - 22YZ^2 + 3Z^3.$$

Proof. The full linear system of degree 3 has dimension 10, and the subsystem passing through the 7 cusps has dimension 3 with a basis in $\mathbb{Q}[X, Y, Z]$. Using LLL-reduction we found a short element which does not pass through any rational points on \mathcal{C} (to simplify the evaluation of the j -map at these points later). \square

Since all cusps have ramification degree 13 under the j -map, a possible choice for the denominator d of the j -map is to take the 13th power of this cubic.

Next we turn to the numerator $n(X, Y, Z)$, which is a polynomial of degree 39. The idea is to consider an arbitrary degree 39 polynomial in the q -expansions of the cusp forms f, g, h , and compare it with the known q -expansion of $j \cdot d(f, g, h)$. This gives a system of linear equations which can be solved.

The full linear system of degree 39 has degree 820, but modulo the defining quartic polynomial for \mathcal{C} we can reduce the number needing to be considered to only 154. We chose those monomials in which, if both X and Y occur, then X occurs with exponent 1 or 2, but this is arbitrary.

Now we consider the equation

$$n(X, Y, Z) - j(X, Y, Z) \cdot d(X, Y, Z) = 0,$$

as a q -expansion identity after substituting f, g, h for X, Y, Z . Using 250 terms in the q -expansions (giving a margin to safeguard against error) and comparing coefficients gives 250 equations for the unknown coefficients of $n(X, Y, Z)$. There is a unique solution, which has rational coefficients. Although we have apparently only shown that the equation holds modulo q^{250} , it must hold identically, since we know that there is exactly one solution.

The expression for $n(X, Y, Z)$ we obtain this way is too large to display here (it has 151 nonzero integral coefficients of between 46 and 75 digits), but can easily be used to evaluate the j -map at any given point on the curve \mathcal{C} .

4.3.2 Step 2. Points on $X_{S_4}(13)$

We have not been able to determine the finitely many \mathbb{Q} -points on the curve, though we have found 4 points:

$$\left(-\frac{1}{2} : -\frac{3}{2} : 1\right), (0 : 0 : 1), (0 : 1 : 0), (1 : 0 : 0).$$

By considering the lines between pairs of these rational points, we obtain 12 quadratic points:

$$\begin{aligned} R_1 &= \left(0 : \frac{1 + \sqrt{-39}}{10} : 1\right), R_2 = \left(\frac{3 + \sqrt{13}}{2} : 0 : 1\right) \\ R_3 &= \left(\frac{3 + \sqrt{-39}}{8} : 1 : 0\right), R_4 = \left(\frac{-25 + \sqrt{-299}}{66} : \frac{-25 + \sqrt{-299}}{22} : 1\right) \\ R_5 &= \left(\frac{1 + \sqrt{-13}}{2} : 1 : -(1 + \sqrt{-13})\right), R_6 = \left(\frac{97 + \sqrt{-6383}}{84} : 1 : -\frac{2}{3}\right) \end{aligned}$$

and their Galois conjugate points. We have also considered tangent lines at the rational points, which gives 4 additional quadratic points on the curve, but we omit them here, because none of them are defined over $\mathbb{Q}(\sqrt{13})$.

4.3.3 Step 3. Evaluate j at these points

Since we are mainly interested in $\mathbb{Q}(\sqrt{13})$ -points on the curve, we consider only the 4 rational points, as well as the point denoted R_2 above, and its Galois conjugate. We evaluate the j -map at these 6 points, and hence obtain the 5 j -invariants displayed at the beginning of this chapter, and zero, which we may ignore; indeed, an elliptic curve with j -invariant 0 has CM by the ring of integers of $\mathbb{Q}(\sqrt{-3})$; 13 splits in this ring, so the mod-13 Galois image must be contained in the normaliser of a split Cartan subgroup, and hence projectively must be contained in a dihedral subgroup, and so cannot be isomorphic to S_4 (and hence its basechange to $\mathbb{Q}(\sqrt{13})$ cannot have projective mod-13 image isomorphic to A_4).

We are guaranteed that, for the rational j -values, $H_{E,13}$ is contained in S_4 , and for the $\mathbb{Q}(\sqrt{13})$ values, that $H_{E,13}$ is contained in A_4 . We now show that we actually have equality.

Lemma 4.3.5. *Let l be a prime for which $X_0(l)$ has genus 0 (that is, $l = 2, 3, 5, 7, 13$). There is an explicit polynomial $F_l(X, Y) \in \mathbb{Z}[X, Y]$ such that, if E/K is an elliptic curve over a number field with $j(E) \neq 0, 1728$, then*

$$H_{E,l} \cong \text{Gal}(F_l(X, j(E))).$$

Proof. The function field of $X_0(l)$ is generated by a single modular function t (the so-called “Hauptmodul”), and classically there is a canonical choice of such, for each l . The j -function is a rational function of t of degree $l+1$ of the form $P(t)/t$, where P is an explicit integral polynomial of degree $l+1$.

Define $F_l(X, Y) = P(X) - YX \in \mathbb{Z}[X, Y]$. Let E/K be an elliptic curve over

a number field, and consider the set of roots of $F_l(X, j(E)) \in K[X]$ over $\overline{\mathbb{Q}}$. As a set, this is in bijection with the set of preimages t of $j(E)$ under the j -map $X_0(l) \rightarrow X(1)$ (which is unramified away from $j = 0$ and $j = 1728$), and hence is in Galois equivariant bijection with the l -isogenies on E . Hence the Galois action on the set of $l + 1$ isogenies is isomorphic to the Galois action on the roots of $F_l(X, j(E))$. \square

Remark 4.3.6. The polynomial $P(t)$ in the above proof is programmed in Sage as `Fricke_polynomial(1)`. For $l = 13$, we have $P(t) = (t^2 + 5t + 13) \cdot (t^4 + 7t^3 + 20t^2 + 19t + 1)^3$, and hence

$$F_{13}(X, Y) = (X^2 + 5X + 13) \cdot (X^4 + 7X^3 + 20X^2 + 19X + 1)^3 - XY.$$

For each of our three rational j -invariants, we may verify that $F_{13}(X, j)$ has Galois group isomorphic to S_4 over \mathbb{Q} , and for the conjugate pair of $\mathbb{Q}(\sqrt{13})$ -values, isomorphic to A_4 over $\mathbb{Q}(\sqrt{13})$. This completes the proof of Theorem 4.0.9.

4.4 Modular curves of level 13 and genus 3

Over the complex numbers, there are precisely 3 modular curves of level 13 and genus 3; they are $X_s(13)$, $X_{ns}(13)$, and $X_{S_4}(13)$; see for example the table of [CP03]. Observe that all of these curves have models over \mathbb{Q} .

In her recent work [Bar12a], [Bar12b], Burcu Baran proved, in two different ways, that the curves $X_s(13)$ and $X_{ns}(13)$ are in fact \mathbb{Q} -isomorphic. Her first proof in [Bar12a] was computational; she computed models of both curves and showed that they give isomorphic curves. Her second proof was more conceptual, establishing that the Jacobians $J_s(13)$ and $J_{ns}(13)$ are isomorphic, with an isomorphism preserving the canonical polarisation of both Jacobians; the Torelli theorem then gives the result.

The \mathbb{Q} -points on $X_s(13)$ have not yet been determined; in fact, as discussed in the final section of [BPR11], $p = 13$ is the *only* prime p for which the \mathbb{Q} -points on $X_s(p)$ have *not* yet been determined, and Baran’s result, linking $X_s(13)$ and $X_{ns}(13)$, may give some indication for why this $p = 13$ case is so difficult: the determination of \mathbb{Q} -points on $X_{ns}(p)$ is known to be a difficult problem.

Another reason for this difficulty is that $J_s(13)(\mathbb{Q})$ is likely to have Mordell-Weil rank 3, which equals the genus, so the method of Chabauty to determine the rational points does not apply. By likely, we mean that the analytic rank of this Jacobian is 3, so under the Birch-Swinnerton-Dyer conjecture, we would have that the Mordell-Weil rank is also 3.

The curves $X_s(13)$ and $X_{S_4}(13)$ are *not* isomorphic, even over \mathbb{C} ; this may be verified using the explicit models of both curves, by computing certain invariants of genus 3 curves and observing that they are different – we are grateful to Jeroen Sijtsling for carrying out this computation.

Nevertheless, their Jacobians are isogenous.

Proposition 4.4.1. *1. There is a \mathbb{Q} -isogeny of degree a power of 13 between $J_s(13)$ and $J_{S_4}(13)$.*

2. These Jacobians are not \mathbb{Q} -isomorphic.

In particular, the Mordell-Weil rank of $J_{S_4}(13)(\mathbb{Q})$ is likely to be 3, the same as the genus of $X_{S_4}(13)$, so again the method of Chabauty for determining the \mathbb{Q} -points on the curve does not apply.

The proof of the Proposition will occupy the rest of the section, and uses many of the ideas in Baran’s paper [Bar12b]. We begin by framing two different aspects from the proof of her Theorem 4.5 in *loc. cit.*

Lemma 4.4.2 (Baran). *Let S be a finite set of primes, p a prime, and $G = \mathrm{GL}_2(\mathbb{F}_p)$. Suppose one has an isomorphism of $\mathbb{Z}_S[G]$ -modules*

$$\bigoplus_i \mathbb{Z}_S[G/H_i] \cong \bigoplus_j \mathbb{Z}_S[G/H'_j], \quad (4.1)$$

where H_i, H'_j are subgroups of G . Then one has \mathbb{Q} -isogenies in both directions

$$\bigoplus_i J(p)_0^{H_i} \sim \bigoplus_j J(p)_0^{H'_j} \quad (4.2)$$

of degree supported only on S . By $J(p)_0^H$, for H a subgroup of G , we mean the identity component of the H -invariants of $J(p)$, which is an abelian variety.

Proof. This is the first half of the proof of Theorem 4.5 in [Bar12b]. Essentially, after clearing denominators in (4.1), one applies the functor $\mathrm{Hom}_{\mathbb{Z}[G]}(-, J(p)(R))$ for varying \mathbb{Q} -algebras R , to obtain an isogeny as in (4.2). We refer to Baran's paper for the details. \square

Remark 4.4.3. The definition of $J(p)$ that Baran uses in the above lemma is slightly different from our definition; she considers the *geometrically disconnected* model of $X(p)$. In this viewpoint, the modular curve $X(p)$ is defined over \mathbb{Q} , is connected over \mathbb{Q} , but over \mathbb{C} , it consists of $p-1$ components, each isomorphic to the “classical component” $\Gamma(p) \backslash \mathcal{H}^*$. Being geometrically disconnected, the Jacobian $J(p)$ is a commutative algebraic group, whose identity component $J(p)_0$ is an abelian variety. $J(p)$ admits an action of $\mathrm{GL}_2(\mathbb{F}_p)$ since the curve $X(p)$ does; hence, the object $J(p)_0^H$ in the above lemma indeed makes sense. This definition of $X(p)$ is also used in the next lemma.

Lemma 4.4.4 (Baran). *Let $H \subset G$, let $H' := H \cap \mathrm{SL}_2(\mathbb{F}_p)$, and let H'^{ab} denote the maximal abelian quotient of H' . Then there is an isogeny*

$$\mathrm{Jac}(X_H(p)) \longrightarrow J(p)_0^H$$

whose degree is a divisor of $\#H'^{ab}$.

Proof. This is the second half of the proof of Theorem 4.5 in [Bar12b]. \square

We introduce some notation to be used in what follows. G will denote $\mathrm{GL}_2(\mathbb{F}_{13})$, B the Borel subgroup of G , and H any subgroup of G . If K is any subgroup of $\mathrm{PGL}_2(\mathbb{F}_{13})$, we denote by $\pi^{-1}(K)$ the pullback of K to G .

We now proceed with the proof of (1) in the Proposition. Let S be the finite set of primes $\{2, 3, 13\}$. One first verifies (for example in Magma) that there is a $\mathbb{Z}_S[G]$ -module isomorphism as follows:

$$\begin{aligned} 2\mathbb{Z}_S[G/\pi^{-1}(S_4)] \oplus \mathbb{Z}_S[G/\pi^{-1}(D_{26})] \oplus \mathbb{Z}_S[G/B] \cong \\ 2\mathbb{Z}_S[G/C_s^+] \oplus \mathbb{Z}_S[G/\pi^{-1}(C_{13} \ltimes C_3)] \oplus \mathbb{Z}_S[G/\pi^{-1}(C_{13} \ltimes C_4)]. \end{aligned} \quad (4.3)$$

We now apply Lemma 4.4.2 to obtain an isogeny between abelian subvarieties of J . For every H appearing in the above relation, one may compute the genus of the corresponding modular curve X_H , and check that, apart from $H = \pi^{-1}(S_4)$ and C_s^+ , the genus is 0; thus, upon passing to the abelian subvarieties as in Lemma 4.4.2, most of the terms vanish, leaving us with a \mathbb{Q} -isogeny

$$(J_0^{C_s^+})^2 \longrightarrow (J_0^{\pi^{-1}(S_4)})^2 \quad (4.4)$$

of degree supported only on S .

We now apply Lemma 4.4.4 to replace $J_0^{C_s^+}$ with J_s and $J_0^{\pi^{-1}(S_4)}$ with J_{S_4} in (6.2). If H is either C_s^+ or $\pi^{-1}(S_4)$, then H'^{ab} is divisible only by primes in S ; thus, we obtain an isogeny

$$J_s^2 \longrightarrow J_{S_4}^2$$

of degree supported only on S . We will work, however, with its dual,

$$\phi : J_{S_4}^2 \longrightarrow J_s^2.$$

Next, we remove the squares in the above formula. We may restrict ϕ to the first component to obtain an isogeny between J_{S_4} and its image, which must be an abelian subvariety A of J_s^2 of dimension 3. It is proved in Section 2 of [Bar12b] that the endomorphism ring $\text{End}_{\mathbb{Q}}(J_s)$ is isomorphic to O_K , the ring of integers of the real cubic subfield K of $\mathbb{Q}(\zeta_7)$; in particular, J_s is simple over \mathbb{Q} (and one may further show that it is in fact absolutely simple, though we will not need this).

We would like to show that A must be J_s . This follows from the following result, whose statement and proof is due to Martin Orr [Orr12]. Note that it applies in our case, since O_K has class number 1.

Lemma 4.4.5 (Martin Orr). *Let A be an abelian variety over a field k whose endomorphism ring is an order in a number field of class number 1. Then the only isomorphism classes of abelian subvarieties of $A \times A$ are 0 , A and $A \times A$.*

Proof. Let B be an abelian subvariety of $A \times A$, not 0 or $A \times A$. Let $R = \text{End}_k A$. Then $\text{Hom}(B, A)$ is an R -module by composition. Since A and B are isogenous, it is a torsion-free R -module of rank 1. Since R is a PID, $\text{Hom}(B, A)$ is isomorphic to R as an R -module. Hence there is some $f : B \rightarrow A$ such that $\text{Hom}(B, A) = Rf$. Let $p, q : B \rightarrow A$ denote the projections onto the two factors of $A \times A$. By the above, p and q both factor through f ; in particular they both vanish on $\ker f$. But $\ker p$ and $\ker q$ have trivial intersection. Hence $\ker f$ is trivial, and f is an isomorphism $B \rightarrow A$. \square

Therefore, we now have an isogeny

$$\phi : J_s \longrightarrow J_{S_4}$$

of degree supported only on S .

The final step to prove (1) is to remove the primes 2 and 3 from the degree of ϕ . As explained in Proposition 5.2 and the preceding discussion in [Bar12b], this

follows from showing that the residual Galois representation $J_s[\mathfrak{p}]$ is irreducible over O_K/\mathfrak{p} for $\mathfrak{p} = (2)$ and (3) . This is proved by Baran in Proposition 5.5 of *loc. cit.*.

We now prove part (2) of the Proposition. Suppose J_s and J_{S_4} were \mathbb{Q} -isomorphic. We may then choose a \mathbb{Q} -isomorphism which is O_K -linear. Applying the arguments of Section 3 of [Bar12b] replacing J_{ns} with J_{S_4} , we arrive at an isomorphism between J_s and J_{S_4} which respects the canonical polarisations of these Jacobian varieties. The Torelli theorem then implies that the curves $X_s(13)$ and $X_{S_4}(13)$ are isomorphic, which is a contradiction.

Remark 4.4.6. It is likely that 13 must divide the order of every isogeny between J_s and J_{S_4} , though we are unable to prove this.

Chapter 5

Computing $S_2(\Gamma_{A_4}(13))$ in 7 Steps

This chapter explicitly computes the space of cuspforms $S_2(\Gamma_{A_4}(13))$, thereby proving Theorem 4.2.1 from the previous chapter.

5.1 Step 1. Identifying our desired space as the invariants of a representation

Since $\Gamma(13) \subset \Gamma_{A_4}(13)$, we obtain

$$S_2(\Gamma_{A_4}(13)) \subset S_2(\Gamma(13)),$$

a 3-dimensional subspace of a 50 dimensional space. Upon this latter 50 dimensional space there is a right action - the *weight 2 slash operator* - of $\mathrm{PSL}_2(\mathbb{Z})$ (since $\Gamma(13)$ is normal in $\mathrm{PSL}_2(\mathbb{Z})$) which, by definition of $S_2(\Gamma(13))$, factors through the quotient $\mathrm{PSL}_2(\mathbb{F}_{13})$, which we recall contains a unique (up to conjugacy) subgroup isomorphic to A_4 . Our desired 3-dimensional space is then the subspace of $S_2(\Gamma(13))$ fixed by A_4 :

$$S_2(\Gamma_{A_4}(13)) = S_2(\Gamma(13))^{A_4};$$

that is, the A_4 -invariant subspace of the $\mathrm{PSL}_2(\mathbb{F}_{13})$ -representation $S_2(\Gamma(13))$.

When we carry out the computation, we will work with an explicit subgroup of $\mathrm{PSL}_2(\mathbb{F}_{13})$ isomorphic to A_4 , namely that generated by the two matrices

$$A = \begin{pmatrix} -5 & 0 \\ 0 & 5 \end{pmatrix} \text{ and } B = \begin{pmatrix} -2 & -2 \\ -3 & 3 \end{pmatrix}.$$

A different choice of A_4 will yield an isomorphic space of cuspforms, which for our application (in computing an equation for $X_{S_4}(13)$) makes no difference. However, the present choice of A_4 is favourable for computational reasons, since it is normalised by the matrix $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$; the congruence subgroup is then said to be of **real type** (see [Cre97, 2.1.3]).

5.2 Step 2. The conjugate representation

Given a congruence subgroup Γ of level 13, denote by $\tilde{\Gamma}$ the following conjugate subgroup of level 13^2 :

$$\tilde{\Gamma} := \begin{pmatrix} 13 & 0 \\ 0 & 1 \end{pmatrix}^{-1} \Gamma \begin{pmatrix} 13 & 0 \\ 0 & 1 \end{pmatrix} \supseteq \Gamma_0(13^2) \cap \Gamma_1(13).$$

In general, $\tilde{\Gamma}$ has level 13^2 ; in particular we have

$$\widetilde{\Gamma(13)} = \Gamma_0(13^2) \cap \Gamma_1(13).$$

We then have the important isomorphism

$$\begin{aligned} S_2(\Gamma) &\longrightarrow S_2(\tilde{\Gamma}) \\ f(z) &\longmapsto f(13z), \end{aligned}$$

which on q -expansions takes $q := e^{2\pi iz/13}$ to q^{13} . The point is that we may work with $S_2(\widetilde{\Gamma})$ instead of $S_2(\Gamma)$ if we like, as we can easily pass between the two; the two spaces are only superficially different.

This is exactly our plan for $\Gamma(13) \subset \Gamma_{A_4}(13)$. We have $S_2(\widetilde{\Gamma_{A_4}(13)}) \subset S_2(\widetilde{\Gamma(13)})$. This latter space is also a representation of $\mathrm{PSL}_2(\mathbb{F}_{13})$; for $a \in \mathrm{PSL}_2(\mathbb{F}_{13})$, we let A be a pullback to $\mathrm{PSL}_2(\mathbb{Z})$ of a , and define, for $F \in S_2(\widetilde{\Gamma(13)})$,

$$a \cdot F := F|_2 \tilde{A} := F|_2 \begin{pmatrix} 13 & 0 \\ 0 & 1 \end{pmatrix}^{-1} A \begin{pmatrix} 13 & 0 \\ 0 & 1 \end{pmatrix}.$$

We then obtain

$$S_2(\widetilde{\Gamma_{A_4}(13)}) = S_2(\widetilde{\Gamma(13)})^{A_4}.$$

Working inside the conjugated space $S_2(\widetilde{\Gamma(13)})$ is better, since its alternative description as $S_2(\Gamma_0(169) \cap \Gamma_1(13))$ is more amenable to the explicit computations we wish to carry out using the computer algebra systems Sage and Magma. The q -expansions are most naturally expressed by redefining q to be $e^{2\pi iz}$.

5.3 Step 3. Identifying the 3 relevant sub-representations

Inside the space $S_2(\Gamma_0(169) \cap \Gamma_1(13))$ we have the space $S_2(\Gamma_0^+(169))$, the subspace of w_{169} -invariants of $S_2(\Gamma_0(169))$. We can compute this space explicitly in Sage. Let $q := e^{2\pi iz}$, $\zeta_7 := e^{2\pi i/7}$, $\zeta_7^+ := \zeta_7 + \zeta_7^{-1}$, and σ a nontrivial Galois automorphism of the field $\mathbb{Q}(\zeta_7^+) = \mathbb{Q}(\zeta_7)^+$. Then an explicit Sage computation yields

$$S_2(\Gamma_0^+(169)) = \langle g, g^\sigma, g^{\sigma^2} \rangle,$$

where

$$g(z) = q - (\zeta_7^+ + 1)q^2 + (1 - \zeta_7^{+2})q^3 + (\zeta_7^{+2} + 2\zeta_7^+ - 1)q^4 + \cdots.$$

These three forms are Galois conjugate newforms. We will denote by a_n the Fourier coefficients of g .

For each $r \in \mathbb{F}_{13}^*$, define the **isotypical component** g_r of g as

$$g_r := \sum_{j \equiv r \pmod{13}} a_j q^j,$$

and consider the \mathbb{C} -span V_0 of these components. Similarly define V_1 and V_2 by replacing g with g^σ and g^{σ^2} respectively. We will show in the coming sections that each V_i is a 12-dimensional sub-representation of $S_2(\widetilde{\Gamma(13)})$ which is irreducible as a $\mathbb{Q}[\mathrm{PSL}_2(\mathbb{F}_{13})]$ -module. We may focus on these three sub-representations, because, as we compute later, each one contains a unique (up to scaling) A_4 -invariant cuspform.

Since we already know that we are looking for three forms, we need not concern ourselves with the other irreducible components of $S_2(\widetilde{\Gamma(13)})$. In fact, the sum $V_0 \oplus V_1 \oplus V_2$, of dimension 36, is the subspace of $S_2(\Gamma_0(169) \cap \Gamma_1(13))$ spanned by the Galois conjugates of the newform g together with their twists by characters of conductor 13. The complementary subspace of dimension 14 is spanned by oldforms from level 13 and their twists. Each of these two subspaces is the base-change of a vector space over \mathbb{Q} which is irreducible as a $\mathbb{Q}[\mathrm{PSL}_2(\mathbb{F}_{13})]$ -module, while the 36-dimensional piece splits as a $\mathbb{Q}(\zeta_7^+)[\mathrm{PSL}_2(\mathbb{F}_{13})]$ -module into three irreducible 12-dimensional subspaces.

Although we discovered these facts computationally, there is an alternative representation-theoretic explanation of these spaces in Burcu Baran's paper [Bar12a], where she shows in Propositions 3.6 and 5.2 of *loc. cit.* that the spaces V_i are irreducible cuspidal representations of $\mathrm{PSL}_2(\mathbb{F}_{13})$.

5.4 Step 4. Computing the action of $\mathrm{PSL}_2(\mathbb{F}_{13})$ upon each sub-representation

$\mathrm{PSL}_2(\mathbb{F}_{13})$ is generated by the two matrices S and T , where

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

However, since we have conjugated the congruence subgroup, the action we need to consider must also be conjugated by the matrix $\begin{pmatrix} 13 & 0 \\ 0 & 1 \end{pmatrix}$. Hence, $\mathrm{PSL}_2(\mathbb{F}_{13})$ acts on $S_2(\widetilde{\Gamma(13)})$ via the matrices \tilde{S} and \tilde{T} :

$$\tilde{S} = \frac{1}{13} \begin{pmatrix} 0 & -1 \\ 169 & 0 \end{pmatrix} \text{ and } \tilde{T} = \begin{pmatrix} 1 & 1/13 \\ 0 & 1 \end{pmatrix}.$$

Observe that the action of \tilde{S} is, up to a scaling that we may ignore, the same as the Fricke involution w_{169} .

Thus, to describe the action of $\mathrm{PSL}_2(\mathbb{F}_{13})$ on each V_i , we will express the action of \tilde{S} and \tilde{T} on each V_i , explicitly as 12×12 matrices.

5.5 Step 5. Computing the action of \tilde{S} and \tilde{T}

We fix $i = 0$; the computation in the other two cases is completely analogous.

To compute the action of \tilde{T} on V_0 , we use the definition directly:

$$\left(g|_2 \begin{pmatrix} 1 & 1/13 \\ 0 & 1 \end{pmatrix} \right) (z) = g\left(z + \frac{1}{13}\right).$$

Recall that a_i is the i th coefficient of g . We then get

$$g\left(z + \frac{1}{13}\right) = \zeta_{13}q - (\zeta_7^+ + 1)\zeta_{13}^2q^2 + \cdots$$

which we can rearrange as

$$\zeta_{13}(a_1q + a_{14}q^{14} + a_{27}q^{27} + \cdots) + \zeta_{13}^2(a_2q^2 + a_{15}q^{15} + \cdots) + \cdots.$$

Thus, in the isotypical basis for V_0 , the action of \tilde{T} is given simply by the 12×12 diagonal matrix

$$\begin{pmatrix} \zeta & & & \\ & \zeta^2 & & \\ & & \ddots & \\ & & & \zeta^{12} \end{pmatrix}$$

where we write ζ for ζ_{13} . In particular, this shows that V_0 is indeed invariant under the action of \tilde{T} .

Computing \tilde{S} directly on the isotypical basis is not so easy, so what we do is change to a basis upon which we can compute it. Instead of the isotypical basis, we take the **twist basis**

$$\langle g \otimes \chi^j : 0 \leq j \leq 11 \rangle,$$

where $\chi : 2 \mapsto \zeta_{12}$ is a fixed generator of the group of Dirichlet characters of conductor 13, and $g \otimes \chi$ denotes the usual twist of g by χ . Note that this twist basis consists entirely of newforms (see [AL78]). Since twisting by χ preserves V_0 and the change of basis matrix $(\chi^j(i))$ (for $0 \leq j \leq 11$ and $1 \leq i \leq 12$) has nonzero determinant, we have shown the following.

Lemma 5.5.1. *Both the isotypical and twist bases are \mathbb{C} -bases for the 12-dimensional*

subspace V_0 of $S_2(\widetilde{\Gamma(13)})$:

$$\langle g \otimes \chi^j : 0 \leq j \leq 11 \rangle = \langle g_j : 1 \leq j \leq 12 \rangle.$$

Recall that the action of \tilde{S} is the same as the Fricke involution w_{169} . It is known (see [AL78]) that w_N acts on newforms F of level N as

$$F|_2 w_N = \lambda_N(F) \cdot \bar{F},$$

where \bar{F} is the newform obtained from the Fourier expansion of F by complex conjugation, and $\lambda_N(F)$ is the Atkin-Lehner pseudoeigenvalue, an algebraic number of absolute value 1 (Theorem 1.1 of [AL78]). In our twist basis, we have

$$\overline{g \otimes \chi^j} = g \otimes \chi^{12-j},$$

so we only need to compute the pseudoeigenvalues associated to $g \otimes \chi^j$ for $0 \leq j \leq 6$; the others may be obtained from these by complex conjugation. Also, the pseudoeigenvalues for $j = 0$ and $j = 6$ are actually eigenvalues, and may be computed directly (for example in Sage); we find that the eigenvalue for $j = 0$ is $+1$, and for $j = 6$ is -1 .

5.6 Step 6. Computing the Atkin-Lehner pseudoeigenvalues

In order to stay consistent with the notation of [AL78], we relabel g to F , and for this section only we let $q = 13$. By $a(q)$ we mean the q th Fourier coefficient of F , which we may check is 0. We may also check that F is not a twist of an oldform of $S_2(\widetilde{\Gamma(13)})$; thus, in the language of [AL78], F is **13-primitive**. We let χ_0 be

the trivial character mod 13, so $\chi_0 = \chi^0$, and we write $\lambda(\chi)$ for the Atkin-Lehner pseudoeigenvalue of $F \otimes \chi$, for χ any character. We let $g(\chi)$ be the Gauss sum of the character χ , with the convention that $g(\chi_0) = -1$.

The main tool to compute $\lambda(\chi^j)$, for $0 \leq j \leq 11$, is Theorem 4.5 in [AL78], which in the present context is as follows.

Theorem 5.6.1 (Special case of Theorem 4.5 of [AL78]). *With the above notation and assumptions, we have, for $0 \leq j \leq 11$,*

$$(-1)^j 12g(\chi^{12-j})\lambda(\chi^j) = \sum_{k=0}^{11} g(\chi^k)g(\chi^{j+k})\overline{\lambda(\chi^k)}.$$

This theorem gives us, for each $0 \leq j \leq 11$, a linear relation among the $\lambda(\chi^k)$. Although there are twelve $\lambda(\chi^k)$, we have in the previous paragraph computed two of them, leaving us with 10. But actually, we have $\lambda(\chi^j) = \overline{\lambda(\chi^{12-j})}$ for $0 \leq j \leq 5$, so we really only have 5 independent unknowns. However, our strategy is, at first, to consider that we indeed have 10 complex unknowns (namely, $\lambda(\chi^j)$ for $1 \leq j \leq 5$ and $7 \leq j \leq 11$) and use the theorem to derive as many linear relations between these 10 unknowns as we can.

Doing this yields 6 independent equations, whose coefficients lie in $\mathbb{Q}(\zeta_{156})$ (the field over which the Gauss sums are defined). One is, however, able to obtain two more independent equations, by applying Theorem 4.5 of Atkin and Li starting not with $F = g$ (as we did previously), but rather with $F = g \otimes \chi^6$. We thus get the following.

Theorem 5.6.2 (Another special case of Theorem 4.5 of [AL78]). *For $0 \leq j \leq 11$, we have*

$$(-1)^{j+1} 12g(\chi^{12-j})\lambda(\chi^{6+j}) = \sum_{k=0}^{11} g(\chi^k)g(\chi^{j+k})\overline{\lambda(\chi^{6+k})}.$$

As previously stated, this yields two more independent equations, giving us a linear system of 8 independent equations in 10 unknowns.

Let $x = \lambda(\chi)$ and $y = \lambda(\chi^2)$. We obtain the following two linear equations in the unknowns x, \bar{x}, y, \bar{y} .

$$c_1\bar{y} + c_2y + c_3x + c_4\bar{x} = c_5 \quad (5.1)$$

$$c_6y + c_7x + c_8\bar{x} = c_9; \quad (5.2)$$

here the c_i are explicit elements of $\mathbb{Q}(\zeta_{156})$. We now use the relations $x\bar{x} = y\bar{y} = 1$. We use (5.2) to eliminate y and \bar{y} from (5.1) to obtain a linear relation between x and \bar{x} ; now using $x\bar{x} = 1$, we obtain a quadratic in x . This quadratic has no root in $\mathbb{Q}(\zeta_{156})$; we need to adjoin $\sqrt{-7}$, so in fact we work in the field $\mathbb{Q}(\zeta_{1092})$; this might seem excessive, but the coefficients of g are anyway in $\mathbb{Q}(\zeta_7)^+$. This quadratic in x tells us that x is one of two values, and x determines all other $\lambda(\chi^j)$.

In order to determine which of the two values x really is, we computed two competing \tilde{S} matrices, and took the one which satisfied the correct relations with \tilde{T} to be the generators of $\mathrm{PSL}_2(\mathbb{F}_{13})$, namely,

$$\tilde{S}^2 = \tilde{T}^{13} = (\tilde{S}\tilde{T})^3 = 1.$$

5.7 Step 7. The cuspforms

We now have matrices giving the action of \tilde{S} on the twist basis, and the action of \tilde{T} on the isotypical basis; a change of basis matrix applied to either of these gives the action of both matrices in terms of the same basis. Write $\rho(S)$ and $\rho(T)$ for the 12×12 matrices giving the action of \tilde{S} and \tilde{T} respectively with respect to the twist basis.

We now compute the A_4 -invariant subspace of V_0 . Recall that our generators of

$A_4 \subset \mathrm{PSL}_2(\mathbb{F}_{13})$ are

$$A = \begin{pmatrix} -5 & 0 \\ 0 & 5 \end{pmatrix} \text{ and } B = \begin{pmatrix} -2 & -2 \\ -3 & 3 \end{pmatrix}.$$

Writing each generator as a word in S and T :

$$A = T^5 S T^{-2} S T^2 S T^5 S T^{-5},$$

$$B = T^4 S T^3 S T^{-3} S,$$

the action of A_4 on $S_2(\widetilde{\Gamma(13)})$ is given by the same words in the matrices \tilde{S}, \tilde{T} :

$$\tilde{A} = \tilde{T}^5 \tilde{S} \tilde{T}^{-2} \tilde{S} \tilde{T}^2 \tilde{S} \tilde{T}^5 \tilde{S} \tilde{T}^{-5},$$

$$\tilde{B} = \tilde{T}^4 \tilde{S} \tilde{T}^3 \tilde{S} \tilde{T}^{-3} \tilde{S}.$$

The action of \tilde{A} and \tilde{B} on our vector space V_0 is given by taking the same words as above, but in $\rho(S)$ and $\rho(T)$; we call the resulting matrices $\rho(A)$ and $\rho(B)$.

Finally, the intersection of the kernels of $\rho(A) - I$ and $\rho(B) - I$ is one-dimensional, spanned by a vector of the coefficients, in the twist basis, of an A_4 -invariant cuspform in V_0 . These coefficients lie in the degree 9 field $\mathbb{Q}(\zeta_7^+, \zeta_{13}^{++})$, where by $\mathbb{Q}(\zeta_{13}^{++})$ we denote the unique cubic subfield of $\mathbb{Q}(\zeta_{13})$. We call this A_4 -invariant form f .

We do not in fact have to repeat the calculation for V_1 and V_2 , because of the following fact. Here we regard the V_i as $\bar{\mathbb{Q}}[\mathrm{PSL}_2(\mathbb{F}_{13})]$ -modules.

Lemma 5.7.1. *Let γ be an element of $\mathrm{PSL}_2(\mathbb{F}_{13})$. The following diagram commutes.*

$$\begin{array}{ccc} V_0 & \xrightarrow{\sigma} & V_1 \\ \gamma \downarrow & & \downarrow \gamma \\ V_0 & \xrightarrow{\sigma} & V_1 \end{array}$$

Proof. Each V_i admits a twist basis, corresponding to g^{σ^i} and its twists under powers of χ . Fixing this twist basis for each V_i , we find that the action of \tilde{S} and \tilde{T} is exactly

the same; this is because the entries in \tilde{S} and \tilde{T} we found for V_0 are invariant under the action of σ . \square

The lemma allows us to conclude that for $i = 0, 1, 2$, the conjugate f^{σ^i} spans the A_4 -invariant subspace of V_i , and hence that $\{f, f^\sigma, f^{\sigma^2}\}$ is a basis of $S_2(\widetilde{\Gamma_{A_4}(13)})$. Our next step is to replace this basis with one defined over a smaller field, namely $\mathbb{Q}(\zeta_{13}^{++})$.

Write f as

$$f = F + \zeta_7^+ G + \zeta_7^{+2} H,$$

where F, G, H have coefficients in $\mathbb{Q}(\zeta_{13}^{++})$. The forms F, G, H form a basis for the same space, with coefficients in the smaller field.

Lemma 5.7.2. *The following two \mathbb{C} -spans are the same:*

$$\langle f, f^\sigma, f^{\sigma^2} \rangle = \langle F, G, H \rangle.$$

Proof. We have

$$\begin{pmatrix} f \\ f^\sigma \\ f^{\sigma^2} \end{pmatrix} = \begin{pmatrix} 1 & \zeta_7^+ & \zeta_7^{+2} \\ 1 & \sigma(\zeta_7^+) & \sigma(\zeta_7^{+2}) \\ 1 & \sigma^2(\zeta_7^+) & \sigma^2(\zeta_7^{+2}) \end{pmatrix} \begin{pmatrix} F \\ G \\ H \end{pmatrix}$$

where the matrix has nonzero determinant. \square

As a final flourish, we apply the following nonsingular transformation

$$\begin{pmatrix} 1 & 4 & 3 \\ -4 & -3 & 1 \\ 6 & -2 & 5 \end{pmatrix}$$

to obtain the following cuspforms (where again $\zeta = \zeta_{13}$) which are a basis for

$$S_2(\widetilde{\Gamma_{A_4}(13)}).$$

$$f = -q + (-\zeta^{11} - \zeta^{10} - \zeta^3 - \zeta^2)q^2 + (\zeta^{11} + \zeta^{10} - \zeta^9 - \zeta^7 - \zeta^6 - \zeta^4 + \zeta^3 + \zeta^2 - 2)q^3 + \dots$$

$$g = (-\zeta^{11} - \zeta^{10} - \zeta^9 - \zeta^7 - \zeta^6 - \zeta^4 - \zeta^3 - \zeta^2 - 1)q + (-\zeta^{11} - \zeta^{10} - \zeta^9 - \zeta^7 - \zeta^6 - \zeta^4 - \zeta^3 - \zeta^2 - 2)q^2 + (-\zeta^{11} - \zeta^{10} - \zeta^3 - \zeta^2 - 1)q^3 + \dots$$

$$h = (\zeta^{11} + \zeta^{10} + \zeta^3 + \zeta^2 + 3)q + (-\zeta^{11} - \zeta^{10} - \zeta^9 - \zeta^7 - \zeta^6 - \zeta^4 - \zeta^3 - \zeta^2 - 3)q^2 + q^3 + \dots$$

This final transformation was chosen retrospectively, and solely for cosmetic reasons; it moves three of the rational points on the curve to $[1 : 0 : 0]$, $[0 : 1 : 0]$, $[0 : 0 : 1]$.

Theorem 4.2.1 now follows immediately, since to obtain a basis for $S_2(\Gamma_{A_4}(13))$ we merely have to replace the value $q = e^{2\pi iz}$ above with $e^{2\pi iz/13}$, as explained in §5.2 above.

Chapter 6

The Local to Global Problem for Torsion - Problem (2)

6.1 Formulation of the problem

Let A be an abelian variety over a number field K , and let $N \geq 2$ be an integer. Suppose that A has a K -rational N -torsion point, and let \mathfrak{p} be a prime of K at which

- A has good reduction;
- the absolute ramification index $e_{\mathfrak{p}}$ satisfies $e_{\mathfrak{p}} < p - 1$;

note that we are excluding only a finite set of primes of K . It is a well-known fact (see, for example, the Appendix in [Kat81]) that the reduction mod \mathfrak{p} map

$$\mathrm{red}_{\mathfrak{p}} : A(K) \rightarrow \tilde{A}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$$

is **injective** on $A(K)_{tors}$; in particular, $\tilde{A}_{\mathfrak{p}}$ admits an $\mathbb{F}_{\mathfrak{p}}$ -rational N -torsion point, for almost all \mathfrak{p} . We may thus say the following.

Lemma 6.1.1. *On abelian varieties over number fields, the global to local principle holds for rational N -torsion points.*

We may now ask if there is a local to global principle.

Question 6.1.2. *Suppose that $\tilde{A}_{\mathfrak{p}}$ has an $\mathbb{F}_{\mathfrak{p}}$ -rational N -torsion point for almost all \mathfrak{p} . Must A have a K -rational N -torsion point?*

The answer is “No”: Take $K = \mathbb{Q}$, and A the elliptic curve 11a2. We have that $\tilde{A}_{\mathfrak{p}}$ has an $\mathbb{F}_{\mathfrak{p}}$ -rational 5-torsion point for almost all \mathfrak{p} , but nevertheless $A(K) = \{0\}$.

This counterexample is explained by the existence of a \mathbb{Q} -isogeny which 11a1 possesses; 11a1 is isogenous to 11a3, which does have a \mathbb{Q} -rational 5-torsion point. Since the numbers $\#\tilde{A}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$ depend only on the isogeny class of A , 11a1 will be a counterexample.

We may however ask if this is the only way the answer to the above question is “No”.

Question 6.1.3 (Improved). *Suppose that $\tilde{A}_{\mathfrak{p}}$ has an $\mathbb{F}_{\mathfrak{p}}$ -rational N -torsion point for almost all \mathfrak{p} . Does there exist an A'/K , K -isogenous to A , which does have a K -rational N -torsion point?*

6.2 Reformulation of the problem - the work of Katz

In [Kat81], Nick Katz addressed this question. Here is a summary of his results.

Theorem 6.2.1 (Katz). *The answer to Question 6.1.3 is*

- “Yes” if $\dim A = 1$;
- “Yes” if $\dim A = 2$ and N is prime;
- “No” in general if $\dim A \geq 3$. Specifically, for every $d \geq 3$ and $N \geq 3$, there exists a d -dimensional A/K which everywhere locally admits a rational

N-torsion point, but which is not isogenous to an abelian variety admitting a rational N-torsion point.

The case of $\dim A = 2$ and N not prime is still open.

Just as Sutherland does, Katz reduces this problem to group theory, in the introduction to his paper. We only give the reformulation for $N = l$ prime; see Katz's paper for the general case, as well as for why the following question is equivalent to Question 6.1.3 above.

Question 6.2.2 (Katz's reformulation in the prime case). *Let A/K be an abelian variety over a number field, and denote by $G_{A,l}$ the image of the mod- l representation. Suppose*

$$\det(1 - g) = 0 \text{ in } \mathbb{F}_l \text{ for all } g \in G_{A,l}.$$

Does it follow that the semisimplification $\bar{\rho}_{A,l}^{s.s.}$ of the mod- l representation contains the trivial representation?

6.3 The case of modular abelian varieties

Our motivation in this chapter is to make progress on the following task.

To find classes of abelian varieties for which the answer to Question 6.2.2 is "Yes".

Recall the class of modular abelian varieties introduced in 3.7. In this section we prove the following using Katz's group theoretic reformulation 6.2.2.

Theorem 6.3.1. *Let $A = A_f/\mathbb{Q}$ be the modular abelian variety associated to a newform f , and let l be a prime of good reduction for A . Then A satisfies the local to global principle for rational torsion points of order l .*

Proof. Let $\rho_{A,l}$ denote the l -adic representation attached to A , $\rho_{f,\lambda}$ the λ -adic representation attached to f , for $\lambda|l$, and let \mathbb{Z}_f denote the ring of integers of \mathbb{Q}_f , the field of Fourier coefficients of f . We have an equality of L -functions

$$L(A, s) = \prod_{\sigma} L(f^{\sigma}, s), \quad (6.1)$$

where σ runs over the embeddings of \mathbb{Q}_f ; indeed, this equality is an equality at each Euler factor. Let d be the dimension of A .

We are in Katz's situation, so we have

$$\det(I - \bar{\rho}_{A,l}(g)) = 0 \text{ in } \mathbb{F}_l \ \forall g \in G_{\mathbb{Q}}.$$

Fix $g \in G_{\mathbb{Q}}$, and consider

$$F(x) := \det(xI - \rho_{A,l}(g))$$

$$G(x) := \det(xI - \rho_{f,\lambda}(g)).$$

F is a monic polynomial of degree $2d$ with \mathbb{Z} -coefficients, and G is a monic polynomial of degree 2 with \mathbb{Z}_f -coefficients. A remarkable fact is that these polynomials are independent of l , respectively λ , as they are “strictly compatible” in the sense of Serre. The equality of L -functions (6.1) gives that

$$F(x) = \prod_{\sigma} (G(x))^{\sigma},$$

where σ varies over the embeddings of \mathbb{Q}_f . We reduce this equation mod l to obtain

$$\bar{F}(x) = \prod_{\sigma} (G(x) \bmod \lambda)^{\sigma},$$

and note that this equality is true for all $\lambda|l$. By the assumption on F , and by definition of G , we get, upon substituting $x = 1$,

$$0 = \prod_{\sigma} (\det(I - \bar{\rho}_{f,\lambda}(g)))^{\sigma},$$

and hence,

$$\forall \lambda|l, \det(I - \bar{\rho}_{f,\lambda}(g)) = 0 \text{ in } \mathbb{F}_{\lambda}.$$

Next, use the universal identity for 2×2 matrices M :

$$\det(1 - M) = 1 - \text{tr}(M) + \det(M),$$

and hence we have that, for all $g \in G_{\mathbb{Q}}$,

$$\text{tr}(\bar{\rho}_{f,\lambda}(g)) = 1 + \det(\bar{\rho}_{f,\lambda}(g)). \quad (6.2)$$

Now we consider the two $G_{\mathbb{Q}}$ -representations

$$\bar{\rho}_{f,\lambda} \text{ and } \mathbf{1} \oplus \det(\bar{\rho}_{f,\lambda}).$$

They clearly have the same determinant, and by (6.2), they have the same trace, so by the Brauer-Nesbitt theorem, their semisimplifications are isomorphic; in particular, the semisimplification of $\bar{\rho}_{f,\lambda}$ contains $\mathbf{1}$. By the decomposition

$$\rho_{A,l} = \bigoplus_{\lambda|l} \rho_{f,\lambda}$$

(see exercise 9.5.2 in [DS05]), we may conclude that the semisimplification of $\bar{\rho}_{A,l}$ also contains $\mathbf{1}$, and the proof is complete. \square

Question 6.3.2. *Consider the class of Jacobians of genus 3 curves over \mathbb{Q} . Does*

this class of abelian varieties satisfy the local to global principle for torsion?

Chapter 7

Conclusion

More questions have been asked in this thesis than have been answered. We wish to collect here those questions which we feel are most worthy of further study.

1. Question 3.3.1, which asked for a description of Hasse curves over degree d fields, is still incomplete for $d = 2$, and for higher values of d is completely open. Related to this is to determine the degree d points on the modular curves $X_s(p)$, which is a known difficult problem.
2. Conjecture 3.3.5 is an interesting problem; even a counterexample to it would be interesting.
3. The investigation of Hasse varieties of higher dimensions is wide open; our section 3.7 are the first small steps in this direction. Progress here would likely require a more explicit understanding of moduli spaces of higher dimensional abelian varieties with level structure; these objects come under the broad umbrella term of “Shimura Varieties of PEL type”.
4. The computations in Chapter 5 ultimately came to computing Atkin-Lehner pseudoeigenvalues. It is possible that our method - both for computing Atkin-Lehner pseudoeigenvalues, and for computing Fourier coefficients of cuspforms of “unusual” congruence subgroups - can be implemented in Sage or Magma.

5. Finding other classes of abelian varieties which satisfy the local to global principle for rational torsion of prime order may be feasible. We are particularly interested in the case of Jacobians of curves.

We have grown accustomed to asking too many questions, and not having enough time to investigate them all, so we postpone any further musings for a rainy day.

Bibliography

- [AL78] A.O.L. Atkin and W. Li. Twists of newforms and pseudo-eigenvalues of W -operators. *Invent. Math.*, 48:221–243, 1978.
- [Ann13] S. Anni. A local-global principle for isogenies of prime degree over number fields. Preprint arXiv:1303.3809, 2013.
- [Bar12a] B. Baran. An exceptional isomorphism between modular curves of level 13. Preprint available at <http://www-personal.umich.edu/~bubaran>, 2012.
- [Bar12b] B. Baran. An exceptional isomorphism between modular curves of level 13 via Torelli’s theorem. Preprint available at <http://www-personal.umich.edu/~bubaran>, 2012.
- [Bar13] F. Bars. On quadratic points of classical modular curves. Preprint available at <http://mat.uab.es/~francesc/>, March 2013.
- [BCP97] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
- [Bea10] A. Beauville. Finite subgroups of $\mathrm{PGL}_2(K)$. In Oscar García-Prada, editor, *Vector Bundles and Complex Geometry*, pages 23–29, 2010.
- [BPR11] Y. Bilu, P. Parent, and M. Rebolledo. Rational points on $X_0^+(p^r)$. Preprint arXiv:1104.4641, 2011.
- [CP03] C.J. Cummins and S. Pauli. Congruence subgroups of $\mathrm{PSL}(2, \mathbb{Z})$ of genus less than or equal to 24. *Exper. Math.*, 12:243–255, 2003.
- [CR94] C. Curtis and I. Reiner. *Methods of Representation Theory, Vol. II*. Wiley-Interscience, 1994.
- [Cre97] J.E. Cremona. *Algorithms for Modular Elliptic Curves*. Cambridge University Press, 1997.
- [Cul12] J. Cullinan. Symplectic stabilizers with applications to abelian varieties. *Int. J. Number Theory*, 08(02):321–334, 2012.
- [Dav11] A. David. Borne uniforme pour les homothéties dans l’image de Galois associée aux courbes elliptiques. *J. Number Theor.*, 131(11):2175–2191, November 2011. Also available at arXiv:1103.3892.

- [DS05] F. Diamond and J. Shurman. *A first course in Modular Forms*. Number 228 in Graduate Texts in Mathematics. Springer-Verlag, Berlin, 2005.
- [Gal96] S. Galbraith. *Equations for Modular Curves*. PhD thesis, University of Oxford, 1996.
- [Hal11] C. Hall. An open-image theorem for a general class of abelian varieties. *Bull. London Math. Soc.*, 43(4):703–711, 2011.
- [Har77] R. Hartshorne. *Algebraic Geometry*. Springer-Verlag, Berlin, 1977.
- [HS91] J. Harris and J. Silverman. Bielliptic curves and symmetric products. *Proc. Amer. Math. Soc.*, 112(2):347–356, 1991.
- [Igu59] J.-I. Igusa. Kroneckerian model of fields of elliptic modular functions. *Amer. J. Math.*, 81:561–577, 1959.
- [Kat81] N. Katz. Galois properties of torsion points on abelian varieties. *Invent. Math.*, 62:481–502, 1981.
- [KM84] N. Katz and B. Mazur. *Arithmetic Moduli of Elliptic Curves*. Princeton University Press, 1984.
- [Lan01] S. Lang. *Introduction to Modular Forms*. Number 222 in Grundlehren der mathematischen Wissenschaften. Springer-Verlag, Berlin, 2001.
- [Lan02] S. Lang. *Algebra*. Number 211 in Graduate Texts in Mathematics. Springer-Verlag, Berlin, 2002.
- [Lig76] G. Ligozat. Courbes modulaires de niveau 11. In J.-P. Serre and D. Zagier, editors, *Modular Functions of One Variable V*, volume 601 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1976.
- [Mai09] R. Maier. On rationally parametrized modular equations. *J. Ramanujan Math. Soc.*, 24:1–73, 2009.
- [Mil08] J. S. Milne. Abelian varieties (v2.00). Available at <http://www.jmilne.org/math/>, 2008.
- [Mil09] J. S. Milne. Algebraic geometry (v5.20). Available at <http://www.jmilne.org/math/>, 2009.
- [Mum74] D. Mumford. *Abelian Varieties*. Oxford University Press, 1974.
- [Orr12] Martin Orr. Private Communication, November 2012.
- [Rib76] K. Ribet. Galois representations attached to eigenforms with nebentypus. In J.-P. Serre and D. Zagier, editors, *Modular Functions of One Variable V*, volume 601 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1976.

-
- [S⁺13] W. A. Stein et al. *Sage Mathematics Software (Version 5.10)*. The Sage Development Team, 2013. <http://www.sagemath.org>.
- [Ser68] J.-P. Serre. *Abelian l -adic representations and Elliptic Curves*. Addison-Wesley, 1968.
- [Ser72] J.-P. Serre. Propriétés galoisiennes des points d’ordre fini des courbes elliptiques. *Invent. Math.*, 15:259–331, 1972.
- [ST68] J.-P. Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math.*, 88(3):492–517, 1968.
- [Ste82] G. Stevens. *Arithmetic on Modular Curves*, volume Progress in Mathematics. Birkhäuser, 1982.
- [Sut12] A. Sutherland. A local-global principle for rational isogenies of prime degree. *J. Théor. Nombres Bordeaux*, 24:475–485, 2012.